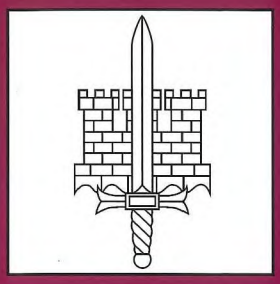


Maanpuolustus-
korkeakoulu

Verkkotaistelu 2020

Taustatutkimus Maavoimien Taistelun kuvat 2020 tutkimukseen

Mika Piiroinen (toim.)

Julkaisusarja 2, N:o 2/2003

Taktiikan laitos

Maanpuolustuskorkeakoulu
Kurssikirjasto

MAANPUOLUTUSKORKEAKOULU
TAKTIIKAN LAITOS
HELSINKI 2003

VERKKOTAISTELU 2020

Taustatutkimus Maavoimien Taistelun kuvat 2020 tutkimukseen

Mika Piiroinen (toim.)

Julkaisusarja 2, N:o 2/2003

Maanpuolustuskorkeakoulu
Kurssikirjasto

100 00 91612

IESBN 951-25-1423-0
ISSN 1238-2752
Edita Prima Oy, Helsinki 2003

LUKIJALLE

Viime vuosina olemme saaneet kuulla ja lukea erilaisista hakkerointitapauksista ja - yrityksistä. Lähes päivittäin ilmenee myös uusia viruksia, joiden avulla pyritään tunkeutumaan niin yritysten kuin yksityishenkilöiden tietojärjestelmiin ja tietokoneisiin tai vain aiheuttamaan mahdollisimman paljon tuhoa ja haittaa. Verkossa on käynnissä koko ajan kaksintaistelu hyökkääjien ja puolustajien välillä.

Taistelukenttä 2020-tutkimushankketta käynnistettäessä havaittiin, että samalla tarjoutuu oiva tilaisuus tutkia verkkosotaa myös hieman laajemmin. Tutkimus päätettiin toteuttaa yhtenä Taistelukenttä 2020 tutkimushankkeen toisen vaiheen osatutkimuksista, jossa esitetään erilaisia taistelukenttien kuvia. Tutkimus liittyy hieman väljemmin koko tutkimushankkeeseen kuin toisen vaiheen muut viisi taistelukenttien kuvaa.

Verkkotaistelu 2020:ssa tavoitteena oli ennen kaikkea kartoittaa näkemyksiä verkkosodankäynnistä. Eri kurssien opetuksen yhteydessä on havaittu, että oppilaiden on hieman hankala hahmottaa kaikkia informaatiosodankäynnin ja verkkosodankäsitteitä ja niiden liittymistä toisiinsa. Tästä syystä tutkimuksen alussa esitetään katsaus verkkosodan käsitteen kehittymisestä. Verkkosodassa sodankäynnin perimmäinen kohde on tieto. Tästä syystä työssä tuodaan esille myös perusteita tiedosta ja tiedon merkityksestä.

Tutkimuksen kahdessa pääluvussa esitetään, miten verkkohyökkäyksiä voitaisiin toteuttaa ja miten niitä vastaan voidaan puolustautua. Johtuen tutkimuksen luonteesta ei artikkeleissa varmastikaan kyetään kattamaan koko aihealuetta. Tämän julkaisun painoarvoa lisää se, että artikkeleiden kirjoittajiksi on saatu arvostettuja siviilipuolen asiantuntijoita ja tutkijoita.

Haluan korostaa, että kirjoitukset eivät edusta puolustusvoimien virallista kantaa. Kirjoituksissa esitetyt näkemykset ja mielipiteet ovat kirjoittajien omia. Toivon, että tämä julkaisu herättää keskustelua ja ajatuksia.

Kiitän artikkeleiden kirjoittajia heidän työstään sekä majuri Mika Piiroista tämän tutkimuksen johtamisesta ja valmiiksi saattamisesta.

Helsingissä 24.6.2003

Taktiikan laitoksen johtaja
Professori Vesa Tynkkynen

SISÄLLYSLUETTELO

Lukijalle **3**

1. Tutkimuksesta – Mika Piiroinen **7**

2. Verkkosodan historia ja käsitteen kehittyminen – Sakari Ahvenainen **12**

3. Tiedon merkitys Suomen puolustamisessa – Tuija Helokunnas, Terhi Laukkanen ja Kalle Viitanen **43**

4. Miten tekisin verkkohyökkäyksen – Mikko Hyppönen **55**

5. Miten verkkotaistelussa puolustaudutaan – Jorma Jormakka **60**

6. Discurssio – Mitä hankkeen jälkeen – Mika Piiroinen **88**

7. Kritiikkipuheenvuoro –Jari Rantapelkonen ja Jukka-Pekka Virtanen **93**

1. VERKKOTAISTELU 2020 - HANKKEESTA

Mika Piiroinen
majuri, viestitaktiikan opettaja
Maanpuolustuskorkeakoulu, Taktiikan laitos

1.1 Yleistä

Viime vuosina olemme voineet lukea sanoma- ja aikakausilehdistä, miten verkkojen kautta on tunkeuduttu yritysten tietojärjestelmiin. Näiden hakkerointitapauksien yhteydessä olemme Taktiikan laitoksella usein pohtineet, että verkkohyökkäystä pitäisi tutkia.

Puolustusvoimissa ei ole juurikaan kirjoitettu verkkosodasta tai – taistelusta. Asiasta ei ole julkaistu tutkimuksia, ei ainakaan julkisia tutkimuksia. Se, että asia mielletään hyvin arkaluonteiseksi ja mahdollisesti turvaluokitukseltaan salaiseksi ei ole ollut kannustamassa asian tutkimusta.

Taistelukenttä 2020-tutkimushankketta käynnistettäessä havaittiin, että samalla tarjoutuu mahdollisuus tutkia myös verkkosotaa. Tutkimushankkeen käynnistäneiden henkilöiden tavoitteena oli saada tietoa verkossa tapahtuvasta "sodankäynnistä". Verkkosota-hanke muuttui työnimeksi Verkkotaistelu 2020. Verkkotaistelu 2020-tutkimus päätettiin toteuttaa yhtenä Taistelukenttä 2020 tutkimushankkeen toisen vaiheen osatutkimuksista. Taistelukenttä 2020:n toisessa vaiheessa TAISTELUKENTTIEN KUVISSA esitetään kuusi pelkistettyä, toisistaan riippumatonta toimintaympäristöä, joissa taistelua oletetaan tulevaisuudessa käytävän. Verkkotaistelu 2020 on yksi näistä kuudesta toimintaympäristöstä.

Tässä artikkelissa pyritään tuomaan esille lähtökohdat Verkkotaistelu 2020-hankkeelle, joka käynnistettiin keväällä 2002 yhteisellä seminaarilla. Alustavat käsikirjoitukset luovutettiin tammikuussa 2003 ja julkaistiin avoimessa tutkimusseminaarissa 5.2.2003.

1.2 Tutkimuksellisia lähtökohtia

Taistelukenttä 2020 tutkimuksessa on muutamia lähtökohtia ja periaatteita, jotka erottavat tutkimuksen monista aikaisemmin puolustusvoimien piirissä tehdyistä tutkimuksista (MpKK TaktL:n tutkimusryhmä 23.5.2001). Kyseiset periaatteet on esitetty Taktiikan laitoksen julkaisussa (Taistelun kuvat 2020 – tutkimussuunnitelma ja kritiikki, Taktiikan

laitoksen julkaisuja julkaisusarja 2, n:o 2/2002), jossa selvitetään koko taistelukenttä 2020-tutkimushanketta.

Miten näitä lähtökohtia ja periaatteita huomioitiin Verkkotaistelu 2020-hankkeessa ?

Verkkotaistelu 2020-työssä kirjoittajiksi pyrittiin samaan oman alansa hyvin tuntevia siviilitutkijoita ja -asiantuntijoita. Kirjoittajat eivät ole sidoksissa Puolustusvoimiin. [AVOIMMUUS] Verkkotaistelun 2020 kirjoittajat omaavat hyvin erilaiset koulutukselliset ja kokemukselliset taustat. Täten he edustavat eri näkemyksiä tutkittavasta asiasta. [MONITIETEISYYS].

Verkkotaistelu 2020-hankkeessa kirjoittajien lähestymistapaa asiaan ei haluttu rajoittaa. Verkkotaistelu 2020 on aiheesta johtuen tutkimus, jossa tieteellisesti perustelemattomienkin visioiden esittäminen on mahdollista. [MONIKASVOISUUS] Alusta saakka lähdettiin liikkelle siitä, että työstä pyritään tekemään julkinen. [JULKISUUS] Tarkoituksena oli herättää keskustelua julkaisemalla työ ja ottaa mukaan julkaistavaan versioon vähintään yksi kriittinen artikkeli.[KRITIIKKI]

Hyvin nopeasti ymmärrettiin, että Verkkotaistelu 2020-hanke on erillinen tutkimushanke Taistelukenttä 2020-tutkimuksessa. Taistelukenttä 2020- hankkeen johtajien kanssa sovittiin, että Verkkotaistelu 2020 on ennen kaikkea avaus keskustelulle ja myöhemmille tutkimuksille.

1.3 Verkkotaistelu 2020 hankkeen tarkoitus

Hankkeen tavoitteena oli luoda ja kartoittaa näkemyksiä verkkotaistelusta ennen kaikkea puolustajan näkökulmasta. Samalla työssä haluttiin pohtia tiedon merkitystä ja vaikutusta puolustusvoimille, koska tiedostettiin, että verkkotaistelun tavoite on taistelu tiedosta.

Tarkoituksena oli, että tutkimus olisi koostunut kuudesta artikkelista. Kaksi kirjoittajaa joutui vetäytymään hankkeesta muista työtehtävistä johtuen. Artikkelien aihealueet pyrittiin muodostamaan niin, että ne täydentäisivät toisiaan. Tutkimuksessa ei haluttu keskittyä sotilaalliseen näkökulmaan, koska verkkotaistelu on koko yhteiskuntaa koskettava asia (yksi työn hypoteesi). Näistä perusteista johtuen valitiin kirjoittajiksi ja aihealueeksi seuraavat asiakokonaisuudet.

1.4 Artikkelit ja niiden kirjoittajat

Verkkosodankäynnin historia ja käsitteen kehittyminen-artikkelin on kirjoittanut everstiluutnantti (evp) Sakari Ahvenainen. Ahvenaista voidaan pitää suomalaisen informaatio- ja johtamissodankäynnin tutkimuksen "pioneerinä". Hän on tutkinut ja kirjoittanut asiasta jo 90-luvulta lähtien. Hänellä on valmistumassa laajempi kirja verkkosodasta. Sakari Ahvenainen toimii myös opettajana Tampereen Teknillisessä Yliopistossa.

Artikkelille asetettiin tavoitteiksi vastata seuraaviin kysymyksiin;

- milloin ja miten käsite verkkosodankäynti (netwar ja/tai cyperwar) on syntynyt ja
- miten käsite on kehittynyt

Mitä yhteiskunnan olisi suojattava verkkosodankäynniltä ? – artikkelin kirjoittajaksi pyydettiin professori Tuija Helokunnasta Tampereen Teknillisestä Yliopistosta. Professori Tuija Helokunnaksella on ollut merkittävä rooli useiden jatko-opintoja suorittavien upseereiden tutkimusten ohjauksessa.

Artikkelin pyrittiin vastamaan seuraaviin kysymyksiin
- mitkä asiat/tekijät (mikä tieto) ovat yhteiskunnan kannalta kriittisiä asioita (nyt, 10 ja 20 vuoden päästä)
- mikä merkitys tiedolla on ja
- mitä asioita yhteiskunnassa on suojattava.

Artikkelissa ovat kirjoittajina Tuija Helokunnaksen lisäksi Terhi Laukkanen ja Kalle Viitanen. Artikkelin kirjoittajat muokkasivat alkuperäistä otsikkoa muotoon; "Tiedon merkitys Suomen puolustamisessa".

Miten tekisin verkkohyökkäyksen ? - artikkelin on kirjoittanut F-Secure Oy:n tutkimuspäällikkö Mikko Hyppönen. Hän on ollut erittäin paljon julkisuudessa esillä nimenomaan viruksien torjuntaan liittyen. Nyt hänelle annettiin tehtäväksi pohtia puolustamisen sijaan hyökkäystä.

Artikkelin avulla pyrittiin vastamaan seuraaviin kysymyksiin;
- miten verkkohyökkäys Oy Suomi Ab:ta (joku isohko ja Suomen kannalta merkittävä yritys) vastaan kannattaisi tehdä nyt ja tulevaisuudessa
- miten verkkohyökkäys kannattaisi organisoida ja toteuttaa ja
- mitkä olisivat verkkohyökkäyksen kohteita eri vaiheissa.

Työ päätettiin toteuttaa myöhemmin esitettävien skenaarioiden pohjalta.

Miten verkkotaistelussa puolustaudutaan ? – artikkelin kirjoittajaksi pyydettiin professori Jorma Jormakkaa. Professori Jormakka työskentelee professorina niin Teknisellä korkeakoululla kuin Maanpuolustuskorkeakoulussa.

Artikkelin avulla pyrittiin vastamaan seuraaviin kysymyksiin;
- miten verkkohyökkäys Oy Suomi Ab:ta vastaan voitaisiin torjua nyt ja tulevaisuudessa
- miten verkon puolustaminen kannattaisi organisoida ja toteuttaa ja
- mitä toimenpiteitä verkkopuolustus edellyttää

Tutkimuksen lopuksi päätettiin kirjoittaa synteesi; **Mitä verkkotaistelusta on opittavaa ?** Synteesin kirjoitti majuri Mika Piiroinen, joka on toiminut myös koko hankkeen vastuuhenkilönä. Mika Piiroinen toimii Maanpuolustuskorkeakoulun taktiikan laitoksella viestitaktiikan pääopettajana. Artikkelissä pyrittiin tekemään yhteenveto kirjassa esitetyistä asioista ja pohtia mitä verkkotaistelu 2020:sta on opittavaa.

Verkkotaistelu 2020-hankkeeseen haluttiin alusta saakka ottaa mukaan oma kritiikkiryhmä varsinaisen Taistelukenttä 2020-kritiikkiryhmän lisäksi. Tätä varten majuri Mika Piiroinen pyysi majuri Jari Rantapelkosta ja majuri Jukka-Pekka Virtasta kirjoittamaan tutkimukseen kritiikkiartikkelin.

Kritiikkiartikkelin avulla haluttaan korostaa, että verkkotaistelusta ei ole olemassa vain yhtä totuutta. Tämän julkaisun kirjoittajat tiedostavat hyvin, että asiasta voidaan esittää lukuisia muita näkökantoja ja näkemyksia, joita tämän julkaisun kirjoittajat eivät ole omissa artikkeleissaan käsitelleet. Kritiikin mukaanotolla on haluttu edesauttaa keskustelun syntymistä, jota toivottavasti asian tiimoilta käydään.

Majuri Jari Rantapelkonen työskentelee Pääesikunnan johtamisjärjestelmäosastolla informaatiosodankäynnin sektorilla. Jari Rantapelkonen jatko-opiskelee Helsingin Yliopistossa. Rantapelkonen on ollut viime vuosina yksi ahkerimpia upseerikirjoittajia. Jari Rantapelkonen on tullut tunnetuksi ennen kaikkea psykologisen sodankäynnin asiantuntijana. Tältä alalta hän julkaisi tutkimuksen vuonna 2002.

Majuri Jukka-Pekka Virtanen toimii viestitaktiikan opettajana Maanpuolustuskorkeakoulun Taktiikan laitoksella. Majuri Virtanen on viimeisen kahden vuoden aikana ollut voimakkaasti kehittämässä informaatiosodankäynnin opetusta.

1. 5 Hypoteesit

Verkkotaistelussa hypoteesina oli kolme erilaista skenaariota. Skeenariot laadittiin yhteistyössä kirjoittajien kanssa. Skenaarioiden laadinnassa käytettiin Delfi-tekniikkaa. Kussakin skenaariossa toteutetaan hyvin valmisteltu verkkohyökkäys Oy Suomi Ab:tä vastaan. Oy Suomi Ab voidaan nähdä joko isona suomalaisena yrityksenä tai koko yhteiskuntana. Kyseinen Oy Suomi Ab käyttää sekä avointa internet- että suljettua intranetratkaisua. Hyökkääjällä on käytössään myös fyysiset menetelmät tunkeutua verkkoon tai tuhota laitteita.

aihe / skenaario	**täsmähyökkäys**	**maan lamautus verkostollisella doktriinilla**	**taloudellinen isku**
hyökkääjä	organisoitu verkottunut liike tai järjestö, analogia 11.9.	vihamielinen kehittynyt valtio, tavanomainen sodankäynti	yritys tai teollisuudenalan etujärjestön iskujoukko
esimerkki	"tämä on varoitus piittaamattomasta suhtautumisesta edustamaamme asiaan" (esim aktivistit/globalisation vastustaja, anti-shell, anti-mcdonalds..)	osa painostusta, erikoisoperaatiota tai strategista iskua, sotilastoimi, Balkan / Afganistan, USA kokeilut	Intelcorp Networks taistelee markkinoista suomalaisten yritysten kanssa
tavoite	vakavan haitan aiheuttaminen merkittävälle yritykselle tai viranomaiselle, varoittava esimerkki muille, painostus tai kosto jostakin toimenpiteestä	pyrkimysten tukeminen maan taivuttamiseksi hyökkääjän tahtoon, merkittävien tietovarastojen tuhoaminen, tavanomainen voitto	haitata yritysten kansainvälistä toimintaa ja heikentää kilpailukykyä

keinot	täsmävirukset, kriittisten tietokantojen muokkaus tai tuhoaminen myös organisaation sisältä käsin, palvelunesto, fyysiset? Hyökkääjät osaavia, motivoituneita ja korkeasti koulutettuja siviilejä. tiedonkeruu, exploitit, rootkittejä, mobiilin koodin käyttö, DoS hyökkäys, virukset, madot ja trojalaiset	kaikki mahdolliset ml COTS-pommit ja takaportit, palvelimien fyysinen tuhoaminen ja avainhenkilöiden eliminointi, verkostollinen tietotekniikka, uudet organisaatiomuodot, informaatiosodankäynti, nopea taistelutempo, vaikutuksen synkronointi. Tietohyökkäyksen valmistelu tai taustatyö on alkanut jo vuosia/ vuosikymmeniä aiemmin esim piilottamalla toimintoja massaohjelmistoihin. Elso-menetelmät ? HPM-aseet ?	kansainvälisen tietoliikenteen haittaaminen, verkkoruuhkat, telekommunikaatio-katkokset, propaganda, psykologiset operaatiot
aikajänne	koordinoitu valmistelu, raju lyhytaikainen isku, informaatioarvon hyväksikäyttö, ei jatkovaikutuksia	pitkäaikainen systemaattinen valmistelu, asevirukset, ajastettu isku osana kokonaisoperaatiota, vaikutusten lisääminen ja taistelu useita vuorokausia – viikkoja	pitkään jatkuva, kehittyvä, huolella organisoitu salattu toiminta
aiheutuva haitta	välillinen yrityksen päätösten ja vuoksi, pörssiarvo, maastalähtö, taloudelliset tappiot	kokonaisuutta lamauttava osana muita toimia, pahimmillaan koko maan perusteita murtava. Sodan häviäminen?	toiminnan vaikeutuminen, yritysten pako Suomesta
erityispiirre, miksi mukana	pyrkimys rajoittaa vaikutus, yllättävyys, reagointiaika, sisäiset viholliset	pahin uhkamalli? lähimpänä pv:n nykyisiä tehtäviä	perinteisistä uhkakuvista poikkeava, globalisaation mukanaan tuoma uhkakuva
puolustus-voimien mahdollinen rooli	nopea tuki, tilan rajoittaminen, voi myös olla itse kohteena ... osallistuva? Valvova?	ohjeistava, valvova, vastajoukot, täysimittainen oma suojaus ... merkittävä? Keskeinen?	Tarpeen tunnistus? Pitääkö yrityksiä osata suojella / tukea edes jotenkin?

2. VERKKOSODAN[1] HISTORIA JA KÄSITTEEN KEHITTYMINEN

Sakari Ahvenainen
Everstiluutnantti, evp

2.1 Yhteenveto

2.1.1 Tiivistelmä

Verkkosodan (netwar[2]) käsitteen historia ja sen ajalliset merkkipaalut ovat olleet:[3]

1. **Informaatiosodankäyntiin liittyvä asevoimien kybersodan (cyberwar) ja siviiliyhteis-kunnan verkkosodan (netwar) termin esittely 1993 ja verkkosodan strateginen, yhteis-kuntiin liittyvä vaihe.**
2. **Verkostolliseen organisaatioon ja toimintaan liittyvä verkostokeskeisen sodan-käynnin (Network-Centric Warfare, NCW) termin esittely 1998 ja sen kokeilut USA:ssa 1990- luvun lopussa.**
3. **Tietokoneverkkohyökkäyksen (Computer Network Attack, CNA) käsitteen ja organisaation julkaiseminen vuonna 2000.**
4. **USA:n puolustusministeriön raportti "Network-Centric Warfare" USA:n kongressille 27.7.2001**
5. **Uuden verkkoteorian paradigman, uuden perustavaa laatua olevan selitysmallin, skaalavapaan verkon, esittely 2000 - 2002.**

On todennäköistä, että verkkosodan käsite ja siihen sisältyvä toiminta kehittyvät vielä merkittävästi eteenpäin seuraavina vuosikymmeninä. Keskeinen pohja tähän on 2000- luvun ensimmäisten vuosien aikana julkaistu uusi verkkoteorian paradigma, skaalavapaa verkko. Toinen syy kehitykseen on tiedon ja verkon uutuus toiminnan keskipisteenä.

Verkkosota on siis laaja ja edelleen laajeneva termi. Tietokoneverkkosodankäynti on tässä esitetyn mallin mukaan yhdeksäsosa verkkosodan nykyisestä sisällöstä..

2.1.2 Tärkeimmät tulokset

Verkkosota laajasti nähtynä sisältää seuraavat osat:
A. Tekniset verkot (verkkotoiminnan tekninen pohja):
1. Tietokoneverkot
2. Muut tiedonsiirtoverkot
3. Sähköisen joukkoviestinnän verkot
4. Sensoriverkot

B. Ihmissuhdeverkot (primääri vaikuttaja ja vaikuttamisen lopullinen tavoite):
5. Ihmissuhdeverkot

C. Verkko organisaationa (vaikuttamisen voiman organisointimuoto)
6. Verkon organisaatiomuotona (täysin kytketty verkko[4]) ja

E. Verkko vaikuttamisen muotona (vaikuttamisen tyyppi, doktriini):
7. Verkkomuotoisen sodankäynnin tai verkkomuotoisen vihamielisen vaikuttamisen doktriini.

F. Verkko logistiikan pohjana (voiman hankinta, siirto, ylläpito) ja
8. Tuotantotoiminnan, kuljetustoiminnan ja huollon verkottuminen.

G: Verkko tiedon pohjana (tiedon hankinta, käsittely, jakaminen ja käyttö)
9. Internet, simulointi, tietokoneet kompleksisuuden (verkon) hallinnan välineenä

Edellä olevia verkkosodan osia voidaan kaikkia käyttää ainakin kahdella tasolla, ensin siviiliyhteiskunnassa globaalista tasosta yksittäiseen ihmiseen ja toiseksi asevoimissa samoin globaalilta tasolta yksitäiseen ihmiseen. Ilmiö on sama kuin informaatio-sodankäynnissä. Sitä ja verkkomuotoista sodankäyntiä tai verkkomuotoista vihamielistä vaikuttamista voidaan käyttää vaikuttamiseen kaikkialla yksilöstä kulttuureihin. Tämä hämärtää sodankäynnin käsitettä.

Verkkosodan ja sen käsitteen ensimmäinen merkitys oli informaatiosodankäynnin strateginen ulottuvuus, sota yhteiskuntien välillä (netwar). Rinnakkainen termi asevoimien informaatiosodalle, kybersota (cyberwar), esitettiin samassa yhteydessä. Molempien käsitteiden pohjana oli uusi 1980- luvun lopun globaali informaatiotekniikka. Elettiin 1990- luvun alkua (1993).

Informaatiosodankäynnin jatkotutkimus, uusin 1990- luvun informaatiotekniikka (internet) ja siviilisovellutukset kaupankäynnissä, rikollisuudessa ja kolmannessa sektorissa johtivat 1990- luvun puolivälissä verkkojen laajenevaan tutkimiseen organisaatiomuotona ja vaikuttamistapana myös sodankäynnin alueella..

Samalla termiin tuli mukaan toisena merkityksenä tietokoneverkkosodankäynti, joka monesti nähdään verkkosodan ainoana sovellutuksena. Sen pohjana on verkkosodan yksi keskeinen tekninen alusta, (1) tietokoneverkot. Muita teknisiä verkkoja ovat (2) muut tiedonsiirtoverkot (matka-puhelimet, tavalliset puhelimet (fax), satelliittiviestintä), (3) sähköinen joukkotiedotus (radio, TV, satelliitti-TV ja internetin sähköiset joukkotiedotussovellutukset) sekä (4) sensoriverkot (tutkat, ihmiset (HUMINT), internet, satelliitit, joukkotiedotus ja julkisiin lähteisiin perustuva tiedustelu (OSINT)). Teknisten verkkojen pohjalla ovat normaalit ihmissuhdeverkostot, jotka ja joiden takana olevat yksilöt ovat edelleen vaikuttamisen pääkohde ja myös vaikuttamisen primääri lähde. Tekniset verkot ovat laajentaneet, reaaliaikaistaneen ja globalisoineet edellä mainittuja ihmissuhdeverk-

koja. Teknisten verkkojen ja ihmissuhde-verkostojen lisäksi verkkosodan kolmas ulottuvuus on organisaatioiden muuttaminen verkottuneiksi, neljäs ulottuvuus vaikutuksen muuttaminen verkottuneeksi, viides ulottuvuus logistiikan muuttaminen verkottuneeksi ja kuudes, viimeinen ulottuvuus tiedon muuttaminen verkottuneeksi.

Verkkoperusteinen organisaatio sodankäynnin puolella esitettiin julkisuudessa 1990- luvun lopulla (Network-Centric Warfare, NCW). Se oli kolmas verkkosodan määritelmä. Samaan aikaan USA:ssa suoritettiin laajoja kokeiluja verkkoperusteisen organisaation eduista ja haitoista. Uusia verkottuneita periaatteita kokeiltiin ilmeisesti sekä Kosovossa[5] 1999 että Afganistanissa 2001 - 2.

Kokeilujen merkittävät tulokset kulminoituivat USA:n puolustusministeriön raporttiin "Network-Centric Warfare" USA:n kongressille 27.7.2001. Siinä suositeltiin koko USA: n asevoiman uudelleenorganisointia verkostokeskeisen sodankäynnin mukaisesti noin vuosina 2002 - 2025.

Vuonna 2000 USA julkisti, että sen on informaatiosodankäynnin doktriiniin kuuluu hyökkäyksellinen tietokoneverkkosodankäynnin elementti. Se perusti Computer Network Attack (CNA) organisaation. Sen elementit olivat avaruus ja tietokoneosaaminen.[6] Aiemmin vain puolustuksellinen tietokoneverkkosodankäynti oli myönnetty julkisesti olevan osa USA:n sotilaallista doktriinia.

Viimeisin merkittävä etappi verkkosodan alueella on uuden verkkoteorian paradigman, skaalavapaan verkon idean esittäminen vuonna 2002. Se luo uutta pohjaa kaikkien verkkojen ja verkkoperusteisen toiminnan tutkimuksiin ja sovellutuksiin. Skaalavapaan verkon paradigmaa ja sen syntyhistoriaa on esitelty laajemmin liitteessä 1.

Verkkosodan laajasti nähtynä on osa informaation kasvavan merkityksen ymmärtämistä ja siirtymistä luonnollisen kehityksen sekä uusien kokemusten ja tutkimusten kautta kohti kokonaisvaltaista konseptia informaation ymmärtämisessä ja hyödyntämisessä. Luvussa 2.2.2 esitetty käsite "Sodankäynnin toiminnalliset ulottuvuudet" on yksi tapa ymmärtää, mitä tämä kokonaisvaltainen käsitys sodankäynnistä voisi pitää sisällään.

Kyse on tietoajan uuden doktriinin muodostumisesta samalla tavalla kuin koneajan uusi doktriini, salamasota, kypsyi käyttöön noin 50 vuotta auton (polttomoottorin) keksimisen jälkeen vuonna 1939.

Tietokoneverkkosodankäynti on edellä olevassa verkkosodan viitekehyksessä yksi yhdeksäsosa verkkosodan kokonaispotentiaalista.

Tutkimuksen tässä osuudessa on päädytty kybersodan (cyberwar) termin osalta uuteen systematiikkaan (ks. luku "Kybersota"). Syntyy neljä kybersodan, informaatiointensiivisen tietoajan sodan, tyyppiä:

1. Johtamissodankäynti
2. Tietokoneverkkosodankäynti, sota, vihamielinen vaikuttaminen, tietokoneverkoisa, hakkerisota.
3. Simuloitu sodankäynti I, tietokonepelien sodankäynti, ihmisten luoma ja käymä virtuaalinen pelien kybersota ja

4. Simuloitu sodankäynti II, tietokonepelien sodankäynti, tiedon luoma ja käymä virtuaalinen pelien kybersota; tulevaisuuden koneiden tiedon luoma ja käymä virtuaalinen pelien kybersota.

Tutkimuksen tässä osassa esitetään myös vihamielisen vaikuttamisen käsite. Sillä tarkoitetaan vaikuttamista, joka vaikutuksensa puolesta on verrattavissa sodankäyntiin, mutta jossa ei kuolla ja jossa ainetta ei fyysisesti tuhoudu. Verkkosota on vihamielistä vaikuttamista ja verkosto-keskeinen sodankäynti sodankäyntiä. Yleensä vihamielinen vaikuttaminen liittyy yhteiskuntiin ja sodankäynti asevoimiin. Vihamielisen vaikuttamisen käsite on osa sodankäynnin (vaikuttamisen) harmaantumista ja yhä tärkeämpi käsite nykyaikaisen kokonaisturvallisuuden ymmärtämiseen.

Organisaatiotapana verkosto on aina ollut olemassa. Globaalin tietotekniikan kehitys on nostanut sen valta-asemaan kaupallisella puolella ja kolmannessa sektorissa. Nyt verkostosta on tulossa keskeinen toimintapa myös valtionhallinnossa ja sen osana asevoimissa.

Sodankäynnin ja minkä tahansa suuremman kokonaisuuden vallankumouksellinen muutos on aina merkittävä kokonaisuus, jossa muutoksen osatekijöiden välillä muodostuu synergiaa, yhteisvaikutusta. Yksittäinen osa, esim. uusi teknologia, ei saa yksinään merkittävää muutosta aikaiseksi.

Verkkosota ja verkostokeskeinen sodankäynti on verkostollisen vaikuttamistavan ja verkostollisen organisaation nostamista strategian ytimeen. Jälkimmäistä voidaan toteuttaa kaikilla sodankäynnin tasoilla, rauhan ja sodan aikana. Edellistä voidaan toteuttaa siviiliyhteiskunnassa kaikilla tasoilla kulttuureista yksilöihin. Verkostoteorian aivan viime vuosien edistykset antavat mahdollisuuden ymmärtää verkkoja paremmin ja laajemmin kuin aikaisemmat selitysmallit. Voidaan perustellusti puhua verkostoteorian uudesta paradigmasta, uudesta perustavasta selitysmallista. Tämä paradigma liittyy kompleksisuuden hallintaa, sen selittämiseen. Kompleksisuus taas on keskeisesti monimutkaisen takaisinkytkennän ja epälineaarisen vaikutuksen omaavia verkkoja vastakohtana lineaarisille järjestelmille.

2.2 Verkkosodan kehityksen tarkastelun taustamalleista

Verkkosodan ja sen termien kehitystä on tarkasteltu kolmen erilaisen mallin, näkökulman avulla. Ensimmäinen on amerikkalaisen informaatiosodankäynnin tutkijan Martin Libickin informaatiosodankäynnin seitsemän tasoinen luokittelumalli. Toinen on everstiluutnantti (evp) Sakari Ahvenaisen sodankäynnin toiminnallisten ulottuvuuksien kuusitasoinen malli.[7]

Kolmas, määritelmiin liittyvä tarkastelutapa on luvussa 2 käsiteltävä malli. Sen pohjana ovat informaatiosodankäynnin ja verkkosodan määritelmät filosofian tohtori Randall Whitakerin kokoaman aineiston mukaan.

2.2.1 Libickin informaatiosodankäynnin laajempi luokittelu

Informaatiosodankäynnissä voidaan Martin Libickin mukaan erottaa seuraavat muodot:[8]
1. Johtamissodankäynti (Command and Control Warfare, C2W)
2. Tiedusteluperustainen sodankäynti (Intelligence-Based Warfare)
3. Elektroninen sodankäynti, elso (Electronic Warfare, EW)
4. Psykologiset sotatoimet (PSYOP, Psychological Operations)
5. Hakkerisodankäynti (Hacker warfare)
6. Taloudellinen Informaatiosodankäynti (Economical Information Warfare) ja
7. Verkkosota/kybersota (Netwar/Cyberwar).

Johtamissodankäynti on amerikkalaisessa ja suomalaisessa määrittelyssä informaatiosodan-käynnin toteuttamista asevoimilla sodan aikana. Sen keskeiset, mutta ei ainoat elementit ovat salaaminen, harhauttaminen, psykologiset sotatoimet, fyysinen tuhoaminen ja elektroninen sodankäynti. Ne muodostavat integroidun kokonaisuuden ja synergia syntyy informaation kautta.

Tiedusteluperustainen sodankäynti on sodankäynnin tietokoneistamista ja automatisointia, nopeaa reagointia. Se on enemmänkin tiedustelutietojen käyttöä suoraan operaatioihin tai asejärjestelmien ohjaamiseen kuin yleisiksi johtamisen perusteiksi. Strategisen iskun järjestelmät ovat tyypillisesti tiedusteluperustaisen sodankäynnin järjestelmiä. Tiedusteluperusteista sodankäyntiä voidaan sanoa myös automaattiseksi sodankäynniksi. Kysymys on pitkälti juuri automaation ulottamisesta uusien viestijärjestelmien, tietokoneiden ja ohjelmistojen avulla laitteista (tekniikasta) taktiikkaan, operaatiotaitoon ja strategiaan.

Elektroninen sodankäynti on sähkömagneettista säteilyä käyttävien tai lähettävien järjestelmien tiedustelua ja valvontaa ja niihin vaikuttamista sähkömagneettisen spektrin avulla sekä suojautumista näiden järjestelmien vaikutuksilta. Elektroninen sodankäynti jakautuu elektroniseen tukeen, elektroniseen vaikuttamiseen ja elektroniseen suojautumiseen. Näistä elektroninen suojautuminen kuuluu kaikille, joilla on elektroniselle hyökkäys- ja tukitoiminnalle alttiita joukkoja tai laitteita. Elektroninen tuki ja elektroninen vaikuttaminen ovat yleensä erikoiskoulutettujen ja -varustettujen elektronisen sodankäynnin joukkojen vastuulla.[9]

Psykologiset sotatoimet tai psykologinen sodankäynti liittyy informaatioon vaikutusketjussa informaatio – asenne – arvot - käyttäytyminen. Muunnos informaatiosta käyttäytymiseen tapahtuu ihmisessä, pääosin alitajuisten, psykologisten prosessien välityksellä. Psykologisen sodankäynnin sovellutusalueet ovat toiminta kulttuureja, toiminta kansan tahtoa, toiminta joukkojen tahtoa ja etenkin toiminta komentajien tahtoa vastaan[10].

Hakkerisodankäynti on tietoverkoissa tapahtuvaa sodankäyntiä, vihamielistä vaikuttamista tietoverkkojen avulla. Se sisältää toimintaa tietoja ja niiden tallennus-, käsittely- ja siirtojärjestelmiä vastaan. Tietojen osalta kyseeseen tulee tietojen hankinta, manipulointi ja tuhoaminen.

Taloudellinen informaatiosodankäynti on tietojen käyttöä taloudelliseen vaikuttamiseen; informaatiosaarto ja informaatioimperialismi. Informaatiosaarto perustuu ajatukseen,

että informaation keskeytyksetön saanti on yhtä välttämätön kuin materiaalin saanti. Informaatio-saarrossa estetään valtion pääsy kansainvälisiin teleyhteyksiin. Tällöin mm. nykyaikainen kansainvälinen pankkitoiminta on mahdotonta. Informaatiosaarto on väkivallaton vaikuttamisen keino.

Verkkosota on ylimmän tason informaatiosotaa. Se on yhteiskuntien näkemys itsestään ja maailmasta sen ympärillä ja sisältää tämän näkemyksen muokkaamisen diplomatialla, propagandalla, psykologisilla toimilla, poliittisella ja kulttuurisuostuttelulla, soluttautumisella paikalliseen mediaan ja tietokoneverkoihin jne.
Kybersota on vastaavasti "sotaa", jota käydään vain kyberavaruudessa. Sitä ovat hakkerit, viestiliikenteen kuuntelijat, hajasäteilyn tiedustelijat jne. Kybersota ei sisällä suoraa kuolemaa.
Kybersodan osa-alueita ovat informaatioterrorismi, semanttinen hyökkäys, simulointisota ja Gibson- sota[11]. Tyypillisimmillään kybersota on hyökkäys- ja puolustusohjelmistojen itsenäistä taistelua tietokoneissa, tietokoneverkoissa ja tiedonsiirtojärjestelmien tietokoneissa.

2.2.2 Sodankäynnin toiminnalliset ulottuvuudet[12]
2.2.2.1 Malli

Sodankäynnissä on viisi, kuusi eri ulottuvuutta, sellaista toisistaan eroavaa toiminnallista kokonaisuutta, jotka vaikuttavat sodankäyntiin oleellisesti ja esiintyvät sen kaikilla tasoilla kaikkina aikoina. Ne ovat operatiivinen, logistinen, sosiaalinen, teknologinen, organisatorinen ja tiedollinen ulottuvuus.

Operatiivinen taso käsittelee sotavoiman käyttöä, logistinen sen luontia siirtoa ja ylläpitoa, sosiaalinen ihmisiin liittyviä käyttäytymisilmiöitä yksilönä ja suuremman ryhmän osana sekä teknologinen taso teknologiaa sodassa mm kaikkien edellisten tasojen yhteydessä. Organisatorinen taso voidaan nähdä sodankäynnin viidentenä ulottuvuutena sisältäen mm. johtosuhteet ja käskyvallan. Tieto on uusin edellisten rinnalle noussut toiminnallinen ulottuvuus. Tieto käsittää perinteisesti tulkittuna sotatoimien input- tiedon, tiedustelun.

Jokaisessa sodassa on ollut edellä mainitut ulottuvuudet ja tulee olemaan. Se miten eri ulottuvuudet painottuvat eri sodissa, vaihtelee. Joissakin sodissa jokin ulottuvuus on noussut muita merkittävämmäksi. Oleellista on kokonaisuus. Kaikkien sodankäynnin välineiden käytössä tulisi huomioida kaikki edellä esitetyt ulottuvuudet ja erityisesti millaista sotaa valmistaudutaan käymään, mitä vastustajaa vastaan, missä olosuhteissa ja mitkä osatekijät tällöin korostuvat.

Sodankäynnin operatiivinen ulottuvuus on perinteisin sodankäynnin ulottuvuus. Se käsittää sotavoiman käyttöä eri tasoilla. Näitä ovat politiikka, strategia, operaatiotaito ja taktiikka. Mm Clausewitz näki sodan operatiivis- sosiaalisena ilmiönä. Operatiivisen sodankäynnin merkitys on sitä suurempi, mitä lyhyempi sota on. Saksalaiset ja japanilaiset näkivät selvästi ensimmäisen maailmansodan jälkeen, että heidän oli voitettava sota nopeasti operatiivisessa ulottuvuudessa. Jos sodan painopiste siirtyisi logistiseen ulottuvuuteen, heidän voimavaroilla edessä olisi varma tappio. Näin myös kävi. Operatiivinen taso sisältää merkittävän tiedollisen elementin. Se on sodankäynnin järjestelmätieto, jota vasten sodankäynnin input- tietoa, tiedustelua, arvioidaan.

Sodankäynnin logistinen ulottuvuus, kyky luoda ja ylläpitää sotavoimaa, vaikutti ensimmäisen kerran ratkaisevasti sodankäyntiin Amerikan Sisällissodan aikana 1861 - 65. Siinä dominoi pohjois-valtioiden kyky luoda ja ylläpitää lukumääräisesti ylivoimainen sotavoima. Etelän operatiivisesti loistavat kenraalit jäivät pohjoisen massojen jalkoihin.[13] Myös Ensimmäisen ja Toisen Maailmansodan loput olivat logistisen, kulutus- tyyppisen sodankäynnin esimerkkitapauksia. Edellä mainittujen sotien logistinen luonne oli mahdollista vain siten, että kyseiset valtiot kestivät sosiaalisesti tämän tyyppisen sodankäynnin.

Sodankäynti sosiaalinen ulottuvuus käsittää ne yksittäiseen ihmiseen liittyvät ja ihmisten väliset ilmiöt, lähinnä tunteet, jotka syntyvät ihmisessä, tai ihmisten välillä taistelijaparissa, ryhmässä, komppaniassa, suuremmissa joukoissa päätyen aina valtioon, ihmiskuntaan ja maailmankaikkeuteen asti. Sotilaallinen toiminta ei koskaan kohdistu vain aineellisiin voimiin; se kohdistuu aina yhtäaikaa moraalisiin voimiin, jotka antavat sodalle sen voiman (life), eikä näitä kahta voi erottaa[14].

Sodankäynnin teknologinen ulottuvuus käsittää sotavoiman käytössä olevan tekniikkaan liittyvät asiat. Clausewitz toteaa, että koska kaikilla sotaa käyvillä on lähes samanlainen tekniikka, teknologialla ei ole suurempaa merkitystä sodassa. Tämä piti paikkansa aina 1800- luvun puoliväliin saakka. Sitten höyryvoima, rautatiet, lennättimet, takaa ladattavat ja kierteillä varustetut kiväärit ja tykit muuttivat tilanteen.

Sodankäynnin organisatorinen ulottuvuus käsittää mm joukkojen organisaatioon, käskyvaltaan, johtosuhteisiin ja yhteistoimintaan liittyvät asiat. Tämän tason peruskysymys on: Hajautettu vai keskitetty? Merkittävin nykyaikainen organisatorisen sodankäynnin sovellutus on ollut salamasotataktiikan kehittäminen 1920- ja 1930- luvuilla. Siinä panssariaseella, ilmavoimilla ja radioilla luotiin uusi tapa käydä sodankäyntiä. Toisen maailmansodan alkaessa sekä liittoutuneilla että akselivaltioilla oli käytössä täysin sama teknologia. Saksassa kyseiset välineet oli organisoitu panssaridivisiooniksi ja taktisiksi ilmavoimiksi, liittoutuneilla tukemaan jalkaväkeä (panssarivaunu) ja pommittamaan vastustajan teollisuuskeskuksia (ilmavoimat). Tavanomainen sota, sissisota ja terrorismi voidaan nähdä kolmena eri tapana organisoida (sota-)voima. Niillä on omat heikkoutensa ja vahvuutensa.

Sodankäynnin tiedollinen ulottuvuus käsittää perinteisesti tiedon hankinnan (tiedustelun ja valvonnan), tiedon käsittelyn (johtaminen ja esikuntatyön), tiedon välittämisen (viestiyhteydet) sekä tiedon käytön (käskyt, ohjeet ja asevaikutus). Tieto on noussut yhä merkittävämmäksi sodankäynnin teknistyessä, muuttuessa yhä kompleksisemmaksi, nopeutuessa ja laajetessa yhä suuremmalle alueelle. Merkittävä uusi tiedollinen tekijä sodankäynnissä on tietokonetekniikan mukana syntyneet tietokoneet ja niiden yhä ratkaisevampi osuus lähes kaikissa sodankäynnin teknisissä järjestelmissä. Tieto on laajentunut aseiden sisäiseksi osaksi, ei pelkästään niiden ulkoa tapahtuva suuntaamisen osaksi. Tietokoneiden merkittävä kokonaisuus on niiden ohjelmistot usealla eri tasolla. Ohjelmistojen merkitys kasvaa jatkuvasti. USA asevoimien hankinnoista yli puolet menee jatkossa ohjelmistoihin.[15] Ohjelmistot ohittivat autoteollisuuden USA:n taloudessa vuonna 2000 ja nousivat samalla USA:n suurimaksi teollisuudenalaksi. Vuonna 1998 ohjelmistoteollisuus työllisti USA:ssa 807.000 ihmistä.[16]

2.2.2.2. Sovellutus[17]

Salamasota voidaan edellä olevan mallin perusteella nähdä synergisenä kokonaisuutena, jossa yhdistyivät seuraavat toiminnalliset ulottuvuudet:

Teknologisessa ulottuvuudessa keskeisiä elementtejä olivat panssarivaunut, moottoroitu tykistö, kuorma-autot, HF- radio ja ilma-voimat, erityisesti syöksypommittajat (Stuka). Mikään näistä ei ollut erityisen erikoinen teknologisesti. Erikoista (logistisesti) oli kaikkien panssarivaunujen varustaminen radioilla. Teknologia mahdollisti nopeuden ja toiminnan vastustajan syvyydessä. Niiden avulla oli mahdollista sekoittaa vastustajan puolustus koko sen syvyydessä.

Doktriini oli toiminnan ydin. Kehitettiin "uusi" tapa käydä sotaa. Ohuet, selustaan iskevät, saarrostavat syvät "nuolet", joilla vastustajan selusta eristettiin tuhottaviksi alueiksi. Nopeus ja toiminnan korkea tempo olivat aivan oleellisia, samoin tehtävätaktiikka, voiman välttäminen ja iskeminen heikkouksiin. Merkittävää oli myös painopisteajattelu ja sen synnyttämä voiman epätasainen jakautuma taistelukentällä ja sen taas synnyttämä paikallinen ylivoima. Tämän jälkeen kaikki elementit, esimerkiksi sodankäynnin toiminnalliset ulottuvuudet synkronoitiin ideaan.

Organisaation osalta oleellista ja tarpeellista oli panssarivaunujen ryhmittäminen panssari-divisiooniksi, ilmavoimien ja maavoimien yhteistoiminta sekä erikoisjoukkojen ja tavallisten joukkojen selkeät ja yhteisvaikutukseen pyrkivät roolit. Erikoisjoukkoja edustivat panssaridivisioonat sekä moottoroidut jalkaväkidivisioonat ja tavallisia joukkoja jalkaväki-divisioonat. Ilma- ja maavoimien yhteistoimintaa edustivat Luftwaffen tulenjohtaja joka divisioonassa ja taktinen ilma-ase.

Logistiikan keskeinen periaate oli, että mukana oli vain välttämätön huolto. Logistiikka oli tämän doktriiniin saksalaisen sovellutuksen toinen merkittävä heikkous. Ensin Saksalla ei ollut taloudellista pohjaa pitkän maailmansodan voittamiseen. Sodan pitkittyessä edessä olisi siis varma tappio. Toiseksi Saksa pystyi moottoroimaan vain pienen osan joukoistaan. Kolmanneksi salamasotadoktriinin edellyttämä huolto-järjestelmä oli kapasiteetiltaan uskomattoman heikko18.

Sosiaalisessa tai ihmisulottuvuudessa oleellista oli omalla puolella ammattiupseeriston saama yhtenäinen koulutus, samanlainen taktinen ajattelu ja ajattelutapa yleensä sekä niihin perustuva luottamus ja sen mahdollistama nopeus päätöksenteossa sekä alajohtoportaiden itsenäisyys (Auftragstaktik). Vihollisen puolella oli oleellista psykologisen vaikutuksen synnyttäminen nopeuden, shokkivaikutuksen ja selustan sekoittamisen avulla sekä hyökkäämällä viestiyhteyksiä ja johtamispaikkoja vastaan.

Tietoulottuvuus sisälsi ensin kehittyneen ja laajan viestijärjestelmän. Viestitys perustui noin 30.000 sähkömekaanisen Enigma- salakirjoituskoneen antamaan nopeuteen ja varmuuteen HF- viestinnässä. Tästä tuli Enigman murtamisen kautta myös salamasotadoktriinin toinen heikkous logistiikan lisäksi. Toiseksi johtajat olivat edessä tekemässä päätökset joukkojen suuntaamista omien havaintojensa perusteella. Kolmanneksi kattava vastustajan järjestelmää testaava tiedustelu oli myös osa doktriinia, samoin valtava määrä hiljaista yhtenäistä tietoa verrattuna siihen mitä viestitettiin. Neljänneksi vastus-

tajan johtaminen ja viestijärjestelmä olivat keskeisiä maaleja tavoitteena oli niitä vastaan hyökkäämällä ja muilla keinoilla saada selusta sekaisin. Lopulta syntyisi ratkaiseva informaatioylivoima taistelussa selustasta, joka yhdessä toiminnan nopeuden kanssa synnyttäisi edelleen psykologisen vaikutuksen ja sen jälkeen seuraisi koko puolustuksen romahdus.

2.3 Verkkosodan keskeiset termit

Verkkosodan ja verkostokeskeisen sodankäynnin sisällön ja kehityksen ymmärtämiseksi on esitetty seuraavat niihin liittyvien tai niitä sivuavien termien määritelmät:

- Informaatiosodankäynti (Engl. Information Warfare, IW)
- Johtamissodankäynti (Engl. Command and Control Warfare, C2W)
- Kyberavaruus (Engl. Cyberspace)
- Kybersota (Engl. Cyberwar)
- Verkkosota (Engl. Netwar, NW) ja
- Verkostokeskeinen sodankäynti (Engl. Network Centric Warfare, NCW)19

2.3.1 Informaatiosodankäynti

Määritelmien pohjana on käytetty pitkälti fil.tri Randall Whitakerin IW- sivujen määritelmiä niiden termien osalta, joista on useita eri käyttöjä. Whitakerin määritelmät sisältävät noin 40 sivua IW:iin liittyviä määritelmiä ja niitä täydentävät noin 40 sivua lähteitä. Sivustosta puuttuu viimeisin kehitys, eli vuodet 1998 - 2002.20 Tätä ajallista osuutta on täydennetty muualta saadulla aineistolla, mm. Suomesta ja internetistä.

Informaatiosodankäynti:
(1) ilmaisee toimia, jotka ovat kietoutuneet ja päällekkäisiä muihin sotilaallisiin operaatioihin, jotka käyttävät dataa ja tietoa tavanomaisten operaatioiden, kuten esim. johtamisen tukena[21].
(2) Manipuloivat, estävät tai tuhoavat toimet, joihin on ryhdytty salaa tai avoimesti rauhan, kriisin tai sodan aikana, sosiaalisia, poliittisia, taloudellisia, teollisia ja sotilaallisia elektronisia tietojärjestelmiä vastaan.[22]
(3) Toimia, joiden tarkoituksena on saavuttaa informaatioylivoima vaikuttamalla vastustajan informaatioon, informaatiopohjaisiin prosesseihin, informaatiojärjestelmiin ja tietokonepohjaisiin verkkoihin samalla käyttäen (leveraging) ja suojaten omaa informaatiota informaatio-pohjaisia prosesseja, informaatiojärjestelmiä ja tietokonepohjaisia verkkoja.[23]
(4) Näkee informaation erillisenä ulottuvuutena (realm), potentiaalisena aseena ja houkuttelevan maalina.[24]
(5) Laajimmin ymmärrettynä yksinkertaisesti informaation käyttöä kansallisten tavoitteiden saavuttamiseen.[25]
(6) Johtamissodankäyntiä huomattavasti laajempi keinovalikoima, joka tähtää vihollisen mieleen ja tahtoon.[26]
(7) Verkkosodan ja/tai kybersodan komponentti (ja siksi siis osa niitä?).[27] [28]

Informaatiosodankäynti USA:n asevoimien määritelmän mukaan on toimia, joiden tarkoituksena on saavuttaa informaatioylivoima (superiority) vaikuttamalla vastustajan informaatioon, informaatioperustaisiin prosesseihin ja informaatiojärjestelmiin ja samalla suojata omaa informaatiota, informaatio-perustaisia prosesseja ja informaatiojärjestel-

miä.[29] Informaatio-järjestelmät ovat sekä inhimillisiä (ihmiset) että automatisoituja (tietokoneet, ym.). Uusimmat julkiset määrittelyt liittävät informaatiosodankäyntiin tietokoneverkkohyökkäykset, CNA (Computer Network Attack). Niiden osalta katso tarkemmin yllä olevat loppuviite.

Informaatiosodankäynti (Engl. Information Warfare, IW) Suomen asevoimien määritelmän mukaan on normaali-ajan ja poikkeusolojen aikaista toisen valtion yhteiskunnalliseen ja sotilaalliseen päätöksen-tekoon ja toimintakykyyn sekä kansalaisten mielipiteisiin vaikuttamista ja näiltä suojautumista käyttämällä informaatiota ja tiedonkäsittelyä sekä kohteena että aseena.
Informaatiosotaa toteutetaan informaatio-operaatioilla, joilla pyritään saavuttamaan vastustajasta informaatioylivoima. Informaatiosodankäyntiä voidaan käydä yhteiskunnallisin, poliittisin, psykologisin, sosiaalisin, taloudellisin ja sotilaallisin keinoin strategisella, operatiivisella tai taktisella tasolla. Informaatiosodankäyntiä voidaan käydä hyökkäyksellisesti tai puolustuksellisesti. Informaatiosodankäynti on kilpailua informaatiosta ja informaatiojärjestelmistä. Normaaliaikana informaatiosodankäynnissä korostuu tietojärjestelmäsodankäynnin ja psykologisen vaikuttamisen puolustuksellinen toiminta.[30]

USA:n puolustusministeriön määritelmä (2003): Informaatiosodankäynti on informaatio-operaatioita, joita suoritetaan kriisin tai konfliktin aikana, jotta saavutettaisiin tai edistettäisiin erityisiä tavoitteita suhteessa erityiseen vastustajaan tai erityisiin vastustajiin.
Informaatio-operaatio taas on toimia, joilla vaikutetaan vastustajan informaatioon ja informaatiojärjestelmiin samalla suojaten omaa informaatiota ja informaatiojärjestelmiä.[31]

Vanhimpana informaatiosodankäynnin termin esiintymisenä pidetään Thomas P. Ronan tutkimusraporttia "Weapon systems and information war" heinäkuulta vuonna 1976.[32]

2.3.2 Johtamissodankäynti (Engl. Command and Control Warfare, C2W)

Johtamissodankäynti USA:n asevoimien ylimmällä, eli Joint- tasolla on salaamisen (OPSEC), sotilaallisen harhauttamisen, psykologisten sotatoimien (PSYOP), elektronisen sodankäynnin (EW) ja fyysisen tuhoamisen integroitua käyttöä. Kaikkia osa-alueita tukee tiedustelu. Johtamissodankäynnillä kielletään tiedon saanti, vaikeuttaa vähentää tai tuhota vastustajan johtamiskapasiteettia. Samalla suojataan oma johtamiskapasiteetti vastaavilta toimilta. Johtamissodankäynti on informaatiosodankäynnin sovellutus sotilasoperaatioissa ja informaatiosodankäynnin alalaji. Johtamissodankäynti soveltuu sotilasoperaatioiden kaikkiin tyyppeihin. Johtamissodankäynti on sekä hyökkäyksellistä että puolustuksellista.[33]

Johtamissodankäynti on (Suomessa) asevoimien informaatiosodankäynnin sotilaallista toteuttamista poikkeusolojen aikana ja tämän toiminnan rauhanaikaista valmistelua.[34]

USA:n puolustusministeriön määritelmä (2003): Johtamissodankäynti on salaamisen (OPSEC), sotilaallisen harhauttamisen, psykologisten sotatoimien elektronisen sodankäynnin ja fyysisen tuhon integroitua käyttöä. Näitä osa-alueita tukee tiedustelu. Tarkoituksena on kieltää informaatio, vaikeuttaa, vähentää tai tuhota vastustajan johtamiskapasiteettia samalla suojaten vastaavilta toimilta. Johtamissodankäynti on informatio-operaatioiden sovellutus sotilaallisissa operaatiossa.[35]

Johtamissodankäynti (Command and Control Warfare, C2W) on korvannut termin Command and Control Counter Measures, C3CM), joka oli yksi sodankäynnin tukitoimista 1980- luvulla. C2W on sitä vastoin doktriini (Joint Pub 3-13.1), sodankäynnin ydintä 1990- luvulla.[36]

Tämä kuvaa keskeisesti ja tärkeällä tavalla muutosta, jossa informaatio on noussut tukitoimesta sodankäynnin keskiöön.

2.3.3 Kyberavaruus (Engl. Cyberspace) 2.4. Kyberavaruus (Engl. Cyberspace)

Kyberavaruus on: (1) Metaforisesti: Informaatioaktiviteetit tai - kokonaisuudet, jotka sijaitsevat tai tapahtuvat tietoverkoissa ja ovat saavutettavissa tietokoneilla.
(2) Globaali yhteen liitettyjen tietokoneiden ja tiedonsiirtojärjestelmien maailma.[37]
(3) Käsitteellinen ympäristö, jossa elektroninen tiedonsiirto tapahtuu. Virtuaalitodellisuuden avaruus.[38]
(4) Termi, jolla viitataan kokonaiseen kokoelmaan asemia, joihin voidaan päästä elektronisesti. Tietokonejärjestelmän informaatioavaruus tai verkostojen järjestelmä. Metaforinen paikka hakkeroinnissa tai krakkeroinnissa olevan henkilön mielessä.[39]
(5) Termin esitti tieteiskirjailija William Gibson (1984). Tämä on maallikon termi asioille, joista lukuisat informaatiosodankäynnin kirjoittajat käyttävät nimityksiä kybermedia, infosfääri, datasfääri, virtuaalimaailma, virtuaalinen taistelukenttä.[40]

Yllä olevat määritelmät kuvaavat kyberavaruuden informaatiosodankäynnin luonnetta, eli ensin tietokoneverkkoja, joissa ihminen voi liikkua vain näiden verkkojen todellisten fyysisten mahdollisuuksien mm. liitäntöjen, käyttöoikeuksien, hakkerointitietämyksen mukaisesti. Toinen selvästi erilainen käsitys kyberavaruudelle on tietokoneteknologian ihmiselle luoma keino-tekoinen (peli-)todellisuus, jonka kanssa hän voi olla fyysisesti kosketuksissa[41]. Kyberavaruus viittaisi siis kahteen selvästi erilliseen tilanteeseen. Tämä jälkimmäinen kyberavaruus ei ole oikeasti olemassa, mutta ihminen voi olla sen kanssa kosketuksissa, tuntea puristavansa asetta, jota ei ole olemassa, mutta jonka hän tuntemisen lisäksi näkee datakypäränsä välityksellä. Sen sijaan ensin mainittu informaatiosodankäynnin kyberavaruus on oikeasti olemassa, mutta ihminen ei voi sitä tuntea eikä fyysisesti liikkua siinä. Jälleen näillä sodilla olisi selvästi, jopa jyrkästi toisistaan eroavat ominaisuudet. Esimerkiksi Microsoft Encarta 99 Encyclopedia Deluxe Version esittää molemmat edellä mainitut kyberavaruuden sovellutukset[42].

USA:n puolustusministeriön määritelmä (2003): Kyberavaruus on käsitteellinen ympäristö, jossa digitaalista informaatiota viestitetään tietokoneverkkojen yli.[43]

2.3.4 Kybersota (Engl. Cyberwar)

Kybersota on (1) RAND RAND Corporation:n synonyymi informaatiosodankäynnille.[44]
(2) Termiä on käytetty myös päinvastaisesti informaatiosodankäynnin osa-alueen nimenä.[45]
(3) Libicki (1995) kutsuu kybersotaa "taisteluksi virtuaalimaailmassa".[46]
(4) Arquilla and Ronfeldt (1993) käyttävät "kybersotaa" kuvatakseen tietopohjaista konfliktia sotilaallisella tasolla ja rajoittavat termin käyttöä informaatiosodankäynnin strategiaan, jota voitaisiin käyttää korkean teknologian osaajan taholta maahantunkeutujaa

vastaan.[47] Näiden kirjoittajien kybersota on eriävä verkkosodasta. Heillä jälkimmäinen on ei-sotilaallista toimintaa.
(5) Synonyymi automaattiselle sodankäynnille, jossa robotit hoitavat pääosan tappamisesta ja tuhoamisesta ilman suoria käskyjä ihmisiltä. Kyseiset aseet olisivat autonomisia.[48]

Edellisen luvun "Kyberavaruus" mukaan on siis olemassa kahdenlaista sodankäyntiä. Ensin sodankäynti, vihamielinen vaikuttaminen, globaalissa tietokoneverkkojen yhteen liittämässä maailmassa ja toiseksi simuloidussa pelimaailmassa, jossa ei ole mitään todellista, kaikki on vain bittejä kyseisen maailman luoneen tietokoneen muistissa. Nämä bitit on muutettu sovittimen, eli datakypärän ja datahansikkaiden avulla ihmisen aistimaan muotoon. Jälkimmäinen kybersodan muoto voi yhdistyä osin edelliseen, jos pelaajat (pelaajien tietokoneet) ovat yhteydessä toisiinsa olevan tietokoneverkon avulla. Silloin heidän virtuaalista (peli-)kybersotaa voidaan häiritä todellisella informaatiosodankäynnin kybersodalla vaikuttamalla pelimaailmaa luoviin todellisiin tietokoneisiin. Kyseiset sodat ovat siis edellä mainitussa tapauksessa tietyllä tavalla "sisäkkäisiä".

Edellä mainitun lähteen kohdat 1 ja 2 liittyvät lähinnä informaatiosodankäynnin kybersotaan, kohta 3 voisi tarkoittaa sekä pelien virtuaalista ja tietoverkkojen tiedollista kybersotaa ja kohta 4 liittyisi tavanomaiseen sodankäyntiin liittyvään kybersotaan. Kohta 5 tapahtuu todellisuudessa, mutta ei sen kehittyneimmässä versiossa, jossa ihminen ei suoranaisesti vaikuta robottien taisteluun, liity enää mitenkään ihmiseen. Ihminen voi kyllä tässä maailmassa liikkua, esimerkiksi yrittäen tuhota aseellisesti näitä robotteja, joten se ei ole myöskään informaatiosodankäynnin kybersotaa. Kohta 5 voisi sisältyä myös tavanomaisen sodankäynnin kyberulottuvuuteen.

Muodostuu siis neljä kybersotaa. Ensin ne jakautuvat todellinen/virtuaalinen- akselille toimintaympäristön mukaan ja toiseksi ihminen/tieto- akselille toimijan mukaan.. Kybersodankäynti muodot ovat siis seuraavat:

Tyypin 1 kybersota: Todellinen maailma, toimija ihminen (fyysinen)
Tyypin 2 kybersota: Todellinen maailman, toimija tieto (tieto, ohjelmistot)
Tyypin 3 kybersota: Virtuaalinen maailma, toimija ihminen (fyysinen) ja
Tyypin 4 kybersota: Virtuaalinen maailma, toimija tieto (tieto, ohjelmistot)

Tyypin 1 kybersota oman nelikenttänsä äärinurkassa on tavanomaista sodankäyntiä fyysisessä todellisuudessa. Sen ympäristö on todellinen, fyysinen, ja toimija on ihminen. Siis sitä (korkeanteknologian) sotaa, jota ihmiset käyvät esimerkiksi täsmäaseilla bunkkereita tuhotessaan. Se on samaa kuin Arquilla & Ronfieldin cyberwar- sota edellä. Se voisi sisältää myös edellä esitetyn robottien välisen sodan. Siinä on todellinen maailma, jossa toiminta on fyysistä, tosin siitä puuttuu ihminen. Ihminen vaikuttaa siinä lähinnä niiden sääntöjen kautta, jotka robotteihin on ohjelmoitu. Voidaan ajatella, että kyseinen sodankäynnin sovellutus on täsmäaseiden, keinoälyn, käytön laajeneminen laitteista järjestelmiin ja järjestelmien järjestelmiin tai taistelutekniikasta (laitteista) taktiikkaan, operaatiotaitoon ja strategiaan. Tyypin 1 kybersota on myös selvästi johtamissodankäyntiä. Vihamieliseen vaikuttamiseen liittyen kyseinen kybersota on asevoimien ulkopuolista informaatiosodankäyntiä.

Tyypin 2 kybersota on oman nelikenttänsä äärinurkassa informaatiosodankäyntiä tietoverkoissa. Se on suomalaisen määritelmän mukaista tietojärjestelmäsodankäyntiä. Sen ympäristö on todellinen, fyysinen, ja toimija on tieto. Tiedon (virus, mato, takaportti, virustorjuntaohjelma...) takana on aina edelleen ihminen, joka luo kyseisen tiedon rakenteen ja toimintalogiikan.

Tyypin 3 kybersota on oman nelikenttänsä äärinurkassa tietokonepelien virtuaalinen maailma. Sen ympäristö on virtuaalinen, epätodellinen, ja toimija on ihminen. Kyseistä ympäristöä ei ole olemassa kuin tietokoneessa ihmisen aisteille sovitettuna, sovittimena datakypärä tai vastaava, mutta ihminen kokee sen fyysisesti, omilla aisteillaan. Ympäristön realistisuus riippuu tietokoneen aistimanipulaation tasosta. Äärilaitaa aistimanipulaation realistisuudessa edusti Matrix- elokuvassa koneiden (tietokoneen) luoma keinotodellisuus suoraan ihmisten päähän. Todellisuudessa ihmiset olivat valtavissa ihmisviljelmissä, joista maailmaa hallitsevat koneet saivat tarvitsemansa energian.

Tyypin 4 kybersota oman nelikenttänsä äärinurkassa on ongelmallisin. Se on edellisen kohdan perusteella tietokonepelien maailman, jossa toimijana on tieto. Sen ympäristö on virtuaalinen, epätodellinen. Se on tietokoneiden ja ohjelmistojen keskinäistä taistelua, jossa ihminen ei ole läsnä. Sen ympäristön ovat luoneet tietokoneet, alunperin49 ehkä ihmisten määrittämien perussääntöjen mukaisena. Fyysisessä todellisuudessa tätä ympäristöä ei ole. Se ei ole ohjelmistojen kamppailua, koska ohjelmistojen, esimerkiksi virusten ja virustorjuntaohjelmien kamppailu tapahtuu todellisissa koneissa, todellisilla yhteyksillä tiedossa (kybersota typpi 2) . Tämä kybersodan versio 4 esiintyy vasta kun tietokoneet kehittyvät tietoisuuden tasolle.

Kybersodalle (cyberwar) ei ollut USA:n puolustusministeriön internet- sivuilla "Military definitions" määritelmää 3.1.2003

2.3.5 Verkkosota (Engl. Netwar)

(1) Verkkosota (a) Käytetty Cyberwar- termin synonyymina - "konflikti virtuaalisessa maailmassa"[50]
(b) Informaatiosodankäynnin osa-alue[51]
(c) Arquilla and Ronfeldt käyttivät termiä täsmällisemmin, sanoen, että se on "yhteiskuntien tasolla tapahtuvaa ideologista konfliktia, jota käydään osin verkottuneissa tiedonsiirto-järjestelmissä ja joka koskee yhteiskuntien kamppailua matalan intensiteetin konflikteissa sellaisten ei-valtiollisten toimijoiden käyttäminä kuin terroristit tai huumekartellit. He käyttävät termin tätä versiota kuvatakseen taktiikka, jolla pyritään informaatioylivoimaan.[52]

(2) Verkkosota (netwar) on ylimmän tason informaatiosodankäynnin alue: Yhteiskuntien näkemys itsestään ja maailmasta niiden ympärillä ja ko. näkemyksen muokkaaminen diplomatialla, propagandalla, psykologisilla toimilla, poliittisella ja kulttuurisuostuttelulla, soluttautumisella paikalliseen mediaan ja tietokoneverkoihin jne.[53]

Tämä verkkoihin liittyvä sodankäynnin muoto esiintyi siis heti informaatiosodankäynnin käsitteen syntyessä. Verkkosota oli aluksi 1990- luvun alussa informaatiosodankäynnin alalaji, osa sen strategista, ylintä ulottuvuutta. Seuraavassa vaiheessa, 1990- luvun lo-

pussa, verkkosota laajeni sotilaalliseen ulottuvuuteen, syntyi verkostokeskeinen sodankäynti.

Verkkosodalle (netwar) ei ollut USA:n puolustusministeriön internet- sivuilla "Military definitions" määritelmää 3.1.2003.

2.3.6 Verkostokeskeinen sodankäynti (Engl. Network Centric Warfare, NCW)

Verkostokeskeinen sodankäynti on informaatioylivoiman mahdollistava toiminta- (operation) konsepti, joka luo kasvavaa taisteluvoimaa verkottamalla sensorit, päätöksentekijät ja ampujat saavuttamaan jaettu tietoisuus, kasvava päätöksenteon nopeus, suurempi toiminnan nopeus, suurempi kuolettavuus, suurempi eloonjäämistodennäköisyys ja suurempi itsesynkronointi. Oleellista on myös sensorin ja toimijan erottaminen.[54]

Verkostokeskeinen sodankäynti on sodankäyntiä. Jotta voisi ymmärtää, mitä on erilaista verkostokeskeisessä sodankäynnissä ja jotta voisi ymmärtää siihen liittyvää lisääntynyttä taiteluvoimaa, on samanaikaisesti keskityttävä sodankäynnin kolmelle tasolle ja niiden väliseen vuorovaikutukseen Nämä kolme tasoa (domain) ovat informaatiotaso, kognitiivinen taso ja fyysinen taso. Fyysinen taso on paikka, jossa asevoimien tavoite vaikuttaa sijaitsee. Se on taso, jolla isku, suojautuminen ja liike tapahtuvat maanpinnalla, merellä, ilmassa ja avaruudessa. Tämä on taso, jolla fyysiset lavetit ja niitä yhdistävät viestiverkot sijaitsevat. ... Taisteluvoimaa on tavanomaisesti mitattu pääosin tällä tasolla. Informaatiotaso on paikka, jossa informaatio luodaan, sitä manipuloidaan ja jaetaan. Se on paikka, jossa sotilaiden tiedonvälitys tapahtuu. Se on paikka, jossa nykyaikaisten asevoimien johtaminen viestitetään, missä komentajan taisteluajatus (intent) tuotetaan (convey). Informaatio, joka on informaatiotasolla voi heijastaa tai voi olla heijastamatta totuudenmukaisesti todellista (ground) totuutta. Kognitiivinen taso on osallistujien mielessä. Tämä on paikka, jossa käsitykset, tietoisuus, ymmärtäminen, uskomukset ja arvot sijaitsevat ja jossa, ymmärryksen teon seurauksena, päätökset tapahtuvat. Tämä on taso, jolla monet taistelut ja sodat itse asiassa voitetaan tai hävitään. Tämä on immateriaalisen taso: Johtajuus, moraali, yksikön koheesio, koulutus- ja kokemustaso, tilannetietoisuus, ja yleinen mielipide. Tällä tasolla sijaitsee komentajan taisteluajatuksen, doktriinin, taktiikan, tekniikoiden, ja prosessien ymmärtäminen. Perustavaa laatua olevat verkostokeskeisen sodankäynnin piirteet voidaan kuvata joukolla yhtyeenliittyviä linkkihypoteeseja, jotka voidaan organisoida kolmeen luokkaan:

- ensimmäisen luokan hypoteesit käsittelevät verkostoitumisen tasojen, informaation jaon, parantuneen tietoisuuden, parantuneen informaation laadun ja jaetun tilannetietoisuuden välisiä suhteita
- toisen luokan hypoteesit sisältävät ne jotka koskevat jaetun tilannetietoisuuden, ja synkronisoinnin välisiä suhteita, esim. eriasteisten jaetun tilannetietoisuuden ja/tai yhteistyön tai synkronoinnin välisiä suhteita
- kolmannen luokan hypoteesit koskevat synkronisoinnin ja tehtävätehokkuuden välisiä yhteyksiä.55

Verkostokeskeiselle sodankäynnille (Network-Centric Warfare) ei ollut USA:n puolustusministeriön internet- sivuilla "Military definitions" määritelmää 3.1.2003.

Johtopäätökset määritelmistä on esitetty johtopäätösluvussa.

2.4 Pohjaa I: Informaatiosodankäynnin tekninen ja yhteiskunnallinen tausta ja sen syntyminen

Informaatiosodankäynti oli pohja verkkosodan ja verkostokeskeisen sodankäynnin kehittymiselle. Informaatiosodankäynnin kehittymisen pohja taas oli keskeisesti uuden tietoteknologian kehittyminen ja sen mukana tapahtunut informaation nousu sodankäynnin keskeisimmäksi tekijäksi, nousu doktriinin ytimeen.

Informaatiosodankäynnin kehittymisen pohja oli ensin tietokonetekniikan kehittyminen. Sen keskeisin piirre oli mikropiirien kehitykseen liittyvä Mooren laki, eli mikropiirien (ja niihin perustuvien tietokoneiden) tehon kaksinkertaistuminen aina puolessatoista vuodessa 1960- luvulta aina pitkälle 2000- luvun ensimmäiselle vuosikymmenelle.[56] Tietokone kehittyi informaatiota käsitteleväksi laitteeksi aluksi maanosakokonaisuuksista (1940- luku) ja siirtyi asteittain 1990- luvulle tultaessa kertakäyttöiseksi laitteeksi esimerkiksi täsmäaseissa. Tällöin tietokoneen aivoja, mikroprosessoreita, oli jo enemmän kuin ihmisiä maapallolla.[57] Samalla tietokoneen käyttö laajeni laskimesta (computer) lähes kaikkien teknisten laitteiden älykkyyttä edustavaksi ytimeksi. Tämän kaiken tekniikan ytimen ydin oli tieto, ensin tietokoneiden käyttöjärjestelminä ja toiseksi monitasoisina käyttöjärjestelmän päälle rakennettuina sovellusohjelmina (tekstin-, kuvan-, äänen ja liikkuvan kuvan käsittely, tiedonsiirto- ja välitysohjelmat, signaalinkäsittely, tietokonepelit, simulointi, mallintaminen, satojen miljoonien teknisten laitteiden ohjaamiseen käytettävät ohjelmat jne.).

Tietokoneiden (mikropiirien) kehittymisen takana on keskeisesti verkottuneen maailman ilmiö, rekursiivinen viittaus. Se tarkoittaa viittausta takaisin itseensä. Tietokoneiden tapauksessa prosessi oli seuraava: Tietokonetta käytetään tietokoneiden (mikropiirien) suunnitteluun. Tehokkaammalla tietokoneella voidaan suunnitella suurempia, tehokkaampia tietokoneita (mikropiirejä). (Edellisen sukupolven) tietokone viittaa siis (seuraavan sukupolven) tietokoneeseen. Seuraa epälineaarinen kasvu, rekursiivisen viittauksen tyypillinen seuraus. Vertaa Mooren laki yllä.

Informaatiosodankäynnin kehittymisen pohja oli toiseksi tiedonsiirtotekniikan kehittyminen ja siihen liittyvä globalisaatio. Aluksi tietokoneohjattuina puhelinkeskuksina, myöhemmin alueellisina (NMT) ja globaaleina (GSM) matkapuhelinkeskuksina, tietokoneita yhteen kytkevinä modeemeina, tietokoneverkkojen reitittiminä monella tasolla (LAN, MAN ja WAN) sekä globaalina tietokoneverkkojen tietokoneverkkona, internettinä 1990-luvulla.

Tietokonetekniikan käyttöönoton lisäksi merkittäviä uusia ratkaisu tiedonsiirtotekniikassa olivat satelliittiviestintä ja valokaapeliyhteydet. Edellinen tarjosi jo 1960- luvulta globaalin puhelintoiminnan ja TV- välityksen mahdollisuudet ja jälkimmäinen hieman myöhemmin lähes rajattoman tiedonsiirtokapasiteetin.

Kolmas informaatiosodankäynnin kehitykseen keskeisesti vaikuttanut tekijä oli globaalin joukkotiedotuksen kehittyminen. Sen mukana syntyivät mm. kaapelitelevisiotoiminta, satelliitti-televisiotoiminta ja kansainväliset satelliittikanavat (CNN).

Viimeisin ja merkittävien informaatiosodankäyntiin vaikuttanut tekijä on ollut interne-

tin kehittyminen. Se tulee olemaan aivan keskeinen väline informaatiosodankäynnissä, verkko-sodassa ja verkostokeskeisessä sodankäynnissä. Edellä mainittu kehitys merkitsi tiedon-välityksen globalisoitumista ja sen radikaalia halpenemista.

Kun edellä olevaan informaatiosodankäynnin tekniseen taustaan liitettiin doktrinäärinen kehitys, eli informaation nostaminen sodankäynnin tukitoiminnasta sen ytimeen, syntyi ensimmäinen informaatioon perustuva sodankäyntitapa, informaatiosodankäynti.

2.5 Pohjaa II: Verkkosodan tekninen ja yhteiskunnallinen tausta

Verkkosota ja verkostokeskeinen sodankäynti liittyy erityisesti organisaatioihin. USA:n merkittävien informaatiosodankäynnin ja verkkosodan tutkijoiden Arquilla & Ronfield'in mukaan organisaatiomuotoja on neljä: Sukulaisuuteen, hierarkiaan, kaupalliseen kilpailuun ja verkostoihin perustuva. Niillä on jokaisella omat etunsa ja haittansa sekä valtakautensa. Kaikki muodot ovat olleet olemassa ja tulevat olemaan jatkossakin.

Verkkosodan merkittävä pohja on verkostoyhteiskunnan syntyminen. Merkittävin alan tutkija on sosiologi Manuel Castells:
Globalisoitunut, informationaalinen yhteiskunta, uudenlainen tuotannon, vallan ja kokemisen kolmiliitto, jossa informaation tuottaminen, prosessoiminen ja välittäminen ovat niin taloudellisen menestyksen kuin demokratian ja kulttuurisen vaikuttamisen väline on syntynyt kolmen tapahtuman yhteisvaikutuksesta. Nämä ovat:[58]
(1) Tietoteknologia oli dynamo siinä kehityksessä, jossa luonnonvarojen hyödyntäminen on vaihtumassa informaation ja tiedon hyödyntämiseen pohjautuvaan kehitykseen. Teknologinen osaaminen on tietoyhteiskunnan perusta, jota ei voi muulla korvata[59].
(2) Sekä kapitalismi että statismi (sosialismi) joutuivat 1970- luvulla taloudelliseen kriisiin ja alkoivat muotoutua uudelleen. Suuryritysten ydintoiminnat globalisoituivat, kehitettiin vähemmän hierarkkisia organisaatioita ja tuotantotapoja. Hallitukset ryhtyivät poistamaan kaupan ja pääoman liikkuvuuden esteitä. Tämä mahdollisti talouselämän yhä kiihkeämmän kehityksen, jonka kyydistä itä-blokin jähmeät valtiokeskeiset maat armotta putosivat.
(3) Opiskelijaliikkeistä 1960- luvulla lähtenyt yhteiskunnallinen liikehdintä esitti kritiikkiä materialisoitunutta, kulutuskeskeistä yhteiskuntaa kohtaa. Samalla se tuki yksilöllistyvää ja yhä kokeellisemmaksi ja symbolikeskeiseksi muotoutuvaa tekniikan kehitystä.

Laajemmassa historiallisessa perspektiivissä verkostoyhteiskunta edustaa laadullista muutosta inhimillisessä kokemuksessa. Ensimmäinen vaihe oli vuosituhansia Luonnon ylivoima Kulttuuriin. Toinen vaihe oli Valistuksesta alkanut ja järjen riemuvoittoon liittynyt Kulttuurin ylivoima Luonnosta. Olemme astumassa uuteen vaiheeseen, jossa Kulttuuri viittaa Kulttuuriin korvattuaan Luonnon siinä määrin, että Luontoa elvytetään keinotekoisesti kulttuurimuodoksi. ... Tästä syystä informaatio on sosiaalisten organisaatioidemme avainaines ja siksi viestien ja mielikuvien siirto verkkojen välillä muodostavat sosiaalisen rakenteemme keskeisten juonteen.[60]

Uusi verkostotekniikka mahdollistaa uudenlaisen toiminnan. Keskeinen muutos on uuden tekniikan mukana tullut tiedonsiirto- ja tiedonkäsittelytekniikan vallankumouksenomainen globalisoituminen, halpeneminen ja samanaikainen tehon kasvu. Tämän seurauksena uudet verkostolliset organisaatiot, joiden keskeinen vaatimus on suuri[61] tiedonsiirtotarve, tulevat mahdolliseksi.

Verkkosota (netwar) lisäsi informaatiosodankäynnin kehitykseen teknisen ja doktrinäärisen taustan lisäksi organisaatio-opin. Syntyi verkkoperusteisen vaikuttamisen ja sen edellyttämän organisaation, täysin kytketyn verkon nykyaikaiset sovellutukset.

2.6 Verkkosodan strateginen aikakausi 1990 - 1995

Ensimmäisenä verkkosota esiintyi terminä "Netwar" Arquilla & Ronfiedin artikkelissa "Cyberwar is comming!"[62] Sillä tarkoitettiin informaatiosodankäynnin strategista, yhteis-kunnallista, ylintä ulottuvuutta:

"Verkkosota (netwar) on ylimmän tason informaatiosodankäynnin alue: Yhteiskuntien näkemys itsestään ja maailmasta niiden ympärillä ja ko. näkemyksen muokkaaminen diplomatialla, propagandalla, psykologisilla toimilla, poliittisella ja kulttuurisuostuttelulla, soluttautumisella paikalliseen mediaan ja tietokoneverkoihin jne." [63]

2.7 Verkostokeskeisen sodankäynnin kokeilut 1995 - 2002

Verkostokeskeisen sodankäynnin käsitteen syntymisen yhtenä alkusysäyksenä voidaan pitää yksinäisen amerikkalaisen hävittäjä USS Sharkin tuhoutumista Persianlahdella 17.5.1987.[64] Tällöin amerikkalaiset saivat jälleen konkreettisen todisteen yksitäiset sotalaivan haavoittuvuudesta. Tätä haavoittuvuutta pyrittiin jatkossa vähentämään verkottamalla sensorit, päättäjät ja ampujat, hyödyntämällä tieto myös horisontaalisesti, verkottuneesti.

Verkostokeskeinen sodankäynti esiteltiin laajemmalle yleisölle ensimmäisen kerran artikkelissa A. K. Cebrowski, J. J. Garstka:"Network-Centric Warfare; Its Orgin ja Future".[65]

USA:n asevoimat suorittivat 1990- luvun loppupuolella laajoja kokeilua verkostokeskeisen sodankäynnin toimivuudesta. Kokeiluissa hierarkkinen, perinteinen toimintatapa muutettiin jo käytössä olevalla tekniikalla verkottuneeksi. Tulokset olivat hätkähdyttäviä[66].

2.8 Strateginen suositus 2002 - 2025: US DoD:n raportti kongressille:"Network-centric Warfare"

USA:n puolustusministeriö jätti USA:n kongressille raportin "Network-Centric Warfare" 27.7.2001. Raportissa hahmotetaan verkostokeskeisen sodankäynnin kokonaisuus ja ehdotetaan, että siitä muodostuisi USA:n asevoimien keskeisin muutos noin vuosina 2001 - 2025.

USA:n Puolustusministeriön raportti kongressille:"Network Centric Warfare" kuvaa verkostokeskeisen sodankäynnin teoriaa, muutaman vuoden tutkimustuloksia verkostokeskeisen sodankäynnin alueella ja suuntaa, johon asiaa halutaan kehittää.

Verkostokeskeisen sodankäynnin tutkimuksessa on saatu merkittäviä tuloksia 1990- luvun lopulla. Ne nähdään kuitenkin vielä alkusoittona sille, mitä on tulossa: USA asevoimat viedään verkostokeskeisen sodankäynnin periaatteilla runsaan kahden vuosikym-

menen aikana aivan uuteen suuntaan, joka hyödyntää keskeisesti uuden tietotekniikan mahdollisuudet sodankäynnissä. Kyseisessä muutoksessa sodankäynti muuttuu merkittävästi.

Raportin johtopäätökset ovat:

1. Tulevaisuudessa verkko tulee olemaan tärkein yksittäinen taisteluvoiman tekijä.
2. On olemassa merkittävä ja kasvavan kiire poistaa kehityksen esteet.
3. Kehityksen esteiden oikea-aikainen poistaminen (tai lievitys) tulee suuresti mahdollistamaan OSD- tason Muutosviraston kehittää ja sitten avustaa käyttöönotossa Puolustusministeriön toimien siinä muutoksessa, jolla aikaansaadaan Puolustusministeriön verkostokeskeinen muutos.
4. Tarvitaan tavoite saavuttaa tietty verkostokeskeisen kyky tietyssä ajassa.
5. Verkostokeskeinen sodankäynti tarjoaa ennennäkemättömiä lupauksia saavuttaa pitkään haluttuja kykyjä ilman vastaavia resurssilisäyksiä pitkällä aikavälillä.
6. Verkostokeskeisen sodankäynnin ja verkostokeskeisten operaatioiden tulisi olla Puolustusministeriön strategisen muutossuunnitelman kulmakiviä.

2.9 Verkostoteorian uusi paradigma; skaalavapaa verkko

Uudenlaista ymmärtämistä verkostojen perusluonteeseen tarjoaa vuonna 2002 julkaistu verkostoteorian uuden paradigman muodostumista kertova kirja:"Linked; The New Science of Network".[67]

Kirjan mukaan verkostojen teorian historia ulottuu matemaatikko Leonhard Euleriin 1700- luvulle (graph theory). Viime vuosina (1999 - 2002) syntyneen uuden teorian sovellutuksia löytyi matematiikasta, fysiikasta, sosiologiasta, taloustieteestä, biologiasta, epidemiologiasta, kielitieteestä, tieteellisestä kirjoittamisesta, sodankäynnistä, terrorismista, ym.

Vuonna 1959 Erdos'in ja Renyi'in keksimä vanha verkosto- tai verkkoteoria perustui satunnaiseen verkkoon. Siinä oleellista olivat topologia, staattisuus ja satunnaisuus. Sen mukaan verkko oli valmiiksi olemassa ja yhteydet ja solmut olivat satunnaisia. Tästä seurasi mm. se, että solmujen yhteysmäärät olivat tilastollisesti jakautuneita (Poisson). Verkosta löytyi mm. tyypillinen solmu.

Uuden verkostoteorian mukaan verkot elävät ja kehittyvät eivätkä solmut ole tasa-arvoisia. Niiden kehitystä ohjaa keskeisesti (1) kasvu ja (2) houkuttelevuustekijä. Syntyy skaalavapaa malli. Sen solmujen yhteydet muodostava potenssi- (power) lain mukaisen jakautuman. Siinä ei ole tyypillistä solmua. Skaalavapaan mallin oleellisia ominaisuuksia ovat ensin siis kasvu ja houkuttelevuustekijä. Lisäksi niitä luonnehtii (3) hubit, kytkijät (hubs), eli hyvin runsaiden yhteysmäärien solmut. Kytkijät ovat todellisten verkkojen avaintekijät.

Verkon topologian kuvaamisesta ollaan siirrytty sen mekanismin ymmärtämiseen, joka muodostaa verkon dynamiikan. Muodostuu vastaparit staattinen - kasvava, satunnainen - skaalavapaa ja struktuuri - evoluutio

Todelliset verkot ovat hyvin yleisiä maailmassa, monella tieteenalalla. Verkkojen muo-

dostuminen liittyy muodonmuutokseen. Todelliset verkot sisältävät useimmiten seuraavan suurrakenteen: Ensin on pienen lähipiirin voimakkaat ja kaikkia koskevat liitynnät, aliverkko, klusteri. Sitten muodostuu heikot yhteyden muihin klustereihin. Jo keskimäärin noin yhdellä yhteydellä per klusteri, aliverkot verkottuvat superverkoksi, joka alkaa elämään omaa elämäänsä. Heikot yhteydet ovat hyvin tärkeitä. Ensin ne muodostavat superverkon vähillä yhteyksillä. Toiseksi niiden antama tieto on poikkeavaa klusterin homogeenisesta tiedosta.

Superverkosta tullaan aivan keskeiseen asiaan, emergenssiin.68 Sillä tarkoitetaan vaikeasti selitettävän ylätason käyttäytymisen syntymistä lukuisista alatason verkottuneista klustereista. Emergenssi on alhaalta ylös ilmiö. Emergenssi syntyy siis kun suuri määrä yksinkertaisia, verkottuneita ilmiöitä (klustereita) vaikuttaa yhdessä.

Klustereiden sovellutuksia löytyy mm. sosiologiasta, taloudesta, aivoista, biologiasta, fysiikasta ja sodankäynnistä. Sosiologiasta esimerkkejä ovat läheiset ystävät, taloudesta keiretsu- idea Japanin taloudessa, aivoista aivojen noin kaksi miljoonaa suuraluetta ja biologiasta läheiset solut, jotka kommunikoivat kemiallisesti keskenään. DNA:n lisäksi olion kehityksen vaikuttaa siis paikallinen informaatio, solujen kemian yhteen sitoma verkko. Edelleen fysiikasta esimerkkejä ovat jäätyminen ja magneetin muodostuminen. Ensin muodostuu useita atomeja käsittäviä, samalla tavalla "käyttäytyviä" atomiklustereita. Sodankäynnissä prikaatia voidaan pitää noin 1000 klusterina, eli ryhmänä, toimistona, ajoneuvokuntana tai vastaavana. Klusterit on tosin prikaatissa organisoitu yhteen enimmäkseen hierarkkisesti. Sen sijaan huomion arvoista on, että klusterit (ryhmät) ovat sodankäynnissäkin sisäisesti enimmäkseen täysin kytkettyjä verkkoja.

Klusterit ja niistä muodostuva superverkko on globaali/paikallinen- sovellutus. Miksi kyseinen rakenne näkyy niin monessa nykyajan ilmiössä? Klusterien ymmärtäminen on tärkeää monen ilmiön ymmärtämiseksi verrattuna yksittäisen toimijan ymmärtämiseen. Esimerkiksi atomiklusterit ovat aineen käyttäytymisessä tärkeämpiä kuin yksittäiset atomit.

Verkko on hyvin kompleksinen rakenne. Verkko on siis merkittävä osa kompleksisuuden ymmärtämistä. Seuraava suuri haaste, seuraava tieteen vuosisata on nimenomaan kompleksisuuden hallintaa. Tämä viittaa vahvasti fyysikko Heinz Pagelsiin vuodelta 1989. Pagelsin mukaan kompleksisuus on seuraavan 300 vuoden tieteen uusi teema. Kun edelliset kolme vuosisataa selvittiin kaukoputkella ja mikroskoopilla, seuraavat kolme vuosisataa keskeisenä tutkimusvälineenä, kompleksisuuden hallinnan välineenä, käytetään tietokonetta.[69]

Liitteessä 1 on selvitetty skaalavapaan verkkoa tarkemmin sekä arvioitu uuden verkostoteorian merkitystä.

2.10 Johtopäätökset verkkosodan ja sen termien kehityksestä

Tiivistelmä ja tärkeimmät tulokset on esitetty tämän luvun alussa. Tässä esitetään vielä johtopäätökset kahden tarkastellun mallin mukaisesti, ensin informaatiosodankäynnin luokittelusta (Libicki) sekä toiseksi sodankäynnin toiminnallisista ulottuvuuksista (Ahvenainen).

2.10.1 Johtopäätökset määritelmistä ja Libickin luokittelusta

Yhteenvetona luvun kaksi määritelmistä voidaan todeta seuraavaa:
Määritelmiin liittyvät viittaukset ovat kahta lukuun ottamatta 1990- luvulta. Verkostokeskeinen sodankäynti on vain muutaman[70] vuoden takainen termi. Termeissä on kyse uusista ilmiöistä. Määritelmät ovat vakiintumattomia jopa englannin kielessä. Samoja termejä käytetään asioiden yhteydessä, jotka ovat merkittävästi erilaisia, jopa vastakkaisia. Esitetyt informaatiosodankäynnin termit liittyvät globaalien tietokone-, tiedonsiirto- ja tietoverkkojen muodostumiseen ja sodankäyntiin niissä tai niiden avulla.

Sekä verkkosodalla että informaatiosodankäynnillä on siviili- ja sotilassovellutus. Sotilaallinen verkkosota on verkostokeskeistä sodankäyntiä ja sotilaallinen informaatiosodankäynti johtamissodankäynti. Vastaavasti siviiliyhteiskunnan verkkosota on verkkosotaa (!) ja informaatiosodankäynti informaatiosodankäyntiä (!).

Edellä olevan epäselvyyden, kaksinkertaisen nimeämisen poistamiseksi verkkosota ja verkosto-keskeinen sodankäynti voitaisiin luokitella yhteisen termin alle. Esitys kyseiselle termille on verkkoperusteinen vaikuttaminen. Siviiliyhteiskunnan informaatiosodankäynti sen sijaan sisältyy alalajeineen informaatiosodankäynnin kokonaistermin alle.

Kybersodan määrittely toimintaympäristön virtuaalinen/fyysinen- ja toimijan tieto/ihminen- akseleilla antaa mielenkiintoisen ja systemaattisen tavan luokitella ja ymmärtää kybersodan eri versioita. Kyseinen tarkastelu avaa myös ikkunan tulevaisuuteen.

Yhteenveto ja suositus edellä mainituista termeistä on seuraava:

1. Kybersota jakautuisi neljään osaan ensin toimintaympäristön (TY) mukaan todelliseen ja virtuaaliseen ja toiseksi toimijan (To) mukaan ihmiseen ja tietoon.
Syntyisi siis neljä kybersotaa seuraavasti:

- johtamissodankäynti, tavanomaisen sodankäynnin keskeisesti informaatiolla tuettu kybersota (TY = todellinen, To = ihminen)
- tietokoneverkkosodankäynti, sota tai vihamielinen vaikuttaminen tietokoneverkoissa, hakkeri-sota, kybersota tietokoneverkoissa (TY = todellinen, To = tieto)
- simuloitu sodankäynti, tietokonepelien sodankäynti, ihmisten luoma ja käymä virtuaalinen pelien kybersota (TY = virtuaalinen, To = ihminen) ja
- (tulevaisuuden) koneiden luoma ja käymä virtuaalinen pelien kybersota (TY = virtuaalinen, To = tieto).

2. Verkkosodalle ja verkostokeskeiselle sodalle voisi olla oma yhteinen luokittelu: Verkosto-muotoinen vaikuttaminen. Tämä liittyy myös vihamielisen vaikuttamisen termiin. Asevoimilla tapahtuva, kuolemaan ja tuhoon liittyvä vaikuttaminen on selkeästi sodankäyntiä. Mutta mitä on vaikuttaminen, jossa ei kuolla eikä tuhouduta fyysisesti, mutta jonka vaikuttamisen lopputulos on kooltaan rinnastettavissa sodankäyntiin? Tätä vaikuttamista kutsutaan vihamieliseksi vaikuttamiseksi erotukseksi sodankäynnistä.

3. Verkkosota viittaisi keskeisesti verkostojen välityksellä tapahtuvaan vihamieliseen vaikuttamiseen yhteiskunnassa. Sen tasot olisivat ylimmästä, eli yhteiskuntien ja kulttuurien välisestä vihamielisestä vaikuttamisesta aina pienempiin ryhmiin ja organisaatioihin, päätyen yksittäiseen ihmiseen.

4. Verkostokeskeinen sodankäynti (Engl. Network Centric Warfare) viittaisi uuteen tavan-omaisten asevoimien sodankäyntitapaan, jossa keskeisenä on koko toiminnan ja erityisesti organisaation muuttaminen verkko- ja verkostopohjaiseksi. Se olisi tavallaan seuraava askel johtamissodankäynnistä uudenlaiseen vallankumoukselliseen tapaan käyttää "tavanomaista" asevoimaa. Tälle termille ei ole vielä suomalaista virallista määritelmää. Esitys termiksi on siis suora käännös, verkostokeskeinen sodankäynti.

Käytännössä edellä oleva tarkoittaisi Libickin vuonna 1993 esittämään informaatiosodankäynnin jakoon seuraavia muutoksia. Ensin verkkosota (netwar) putoaisi verkkoperusteinen vaikuttamisen alalajiksi ja toiseksi verkostokeskeinen sodankäynti (NCW) tulisi toiseksi verkkoperusteisen sodankäynnin uudeksi alalajiksi. Kolmanneksi asevoimien johtamissodan-käynti siirtyisi kybersodan ensimmäisen alalajin alle. Neljänneksi hakkerisodankäynti (tieto-koneverkkosodankäynti, Computer Network Attack, Defence and Operations (CNA, CND, CNO)) siirtyisi kybersodan toiseksi alalajiksi. Viidenneksi kybersodan kolmanneksi alalajiksi syntyisi ihmisten käymä simuloitu sodankäynti, joka on Cyberwar- termin alalaji jo alkuperäisessä Libickin määrittelyssä ja kuudenneksi kybersodan neljänneksi alalajiksi syntyisi tietokoneiden (tiedon) käymä simuloitu sodankäynti. Tämä kybersodan alalaji puuttuu kaikista informaatiosodankäynnin ja kybersodan määrittelyistä.

Lähtökohta: Libicki 1995	Tulos: Ahvenainen 2002
Informaatiosodankäynnin osa-alueet	**Informaatiosodankäynnin osa-alueet**
1. Johtamissodankäynti	1. –
2. Tiedusteluperusteinen sodankäynti	2. Tiedusteluperusteinen sodankäynti (automaatiosodankäynti)
3. Elektroninen sodankäynti	3. Elektroninen sodankäynti (sensori ja viestiverkot)
4. Psykologinen sodankäynti	4. Psykologinen sodankäynti (ihmissuhde- ja joukkotiedotusverkot)
5. Hakkerisodankäynti	5. –
6. Taloudellinen informaatiosodankäynti	6.Taloudellinen informaatiosodankäynti (taloudelliset verkot)
7. Verkkosota (netwar)/Kybersota	7. Verkkoperustainen sodankäynti (organisaatio ja/tai vaikuttaminen) – 7.1. Verkkosota (netwar) – 7.2. Verkostokeskeinen sodankäynti (NCW) 8. Tietoperustainen sodankäynti, kybersota – 8.1. Johtamissodankäynti – 8.2. Tietokoneverkkosodankäynti (hakker warfare, (CNA, CND, CNO)) – 8.3. Simuloitu sodankäynti I (ihmiset) – 8.4. Simuloitu sodankäynti II (tieto)

Kuva 1: Verkkosodan (netwar) uusi viitekehys

Muodostuu siis kuva 1 mukainen rakenne lähtökohdan (Libicki) ja tässä esitetyn tarkastelun (Ahvenainen) välille. Kuvassa näkyy myös verkkosodan määritelmien mukaiseen jaotteluun liittyvät kymmenen osa-aluetta.

2.10.2 Johtopäätöksiä sodankäynnin toiminnallisten ulottuvuuksien kautta

Sodankäynnin kuuden toiminnallisten ulottuvuuden mukaan informaatiosodankäynnissä on kiinnitetty toistaiseksi huomiota lähinnä seuraaviin ulottuvuuksiin: tekniikka, tieto, doktriini ja ehkä hieman koulutuksen osalta myös sosiaaliseen ulottuvuuteen.

Verkkosota ja verkostokeskeinen sodankäynti on tuonut organisatorisen ulottuvuuden informaatiosodankäyntiin ja on ehkä muuttamassa sodankäyntiä ja vaikuttamista merkittävästi.

Mallin mukaan vielä ei ole kiinnitetty merkittävästi huomiota logistiseen ulottuvuuteen. Samoin sosiaalisessa ulottuvuudessa on vielä paljon parantamista mm. luottamuksen ja koulutuksen osalta. Koulutus on keskeinen keino muuttaa organisaation asenteita, tietoa ja osaamista.

Samoin näyttäisi siltä, että tietoulottuvuuden yleistä arvoa on alettu ymmärtää, mutta sen uudelle merkitykselle ei ole löydetty kokonaisvaltaista näkemystä. Merkkinä tästä on keskustelu tietämyssodankäynnistä (knowledge warfare). Tieto- ja teknisen ulottuvuuden keskeinen tekijä on jatkossa internet.

On siis todennäköistä, että informaatioajan informaatiointensiivinen vaikuttaminen kehittyy edelleen. Oleellisin asia on synergisen, tasapainoisen kokonaisuuden muodostaminen kaikista edellä mainituista kuudesta ulottuvuudesta. Tietoulottuvuus, sosiaalinen ulottuvuus ja logistinen ulottuvuus sisältävät myös todennäköisesti vielä merkittäviä kehittämismahdollisuuksia. Samoin kaiken pohjalla oleva mahdollistaja, tekniikka, kehittyy jatkuvasti.

Oppi salamasotadoktriinista on, että oleellisin muutos on doktriinissa, ajattelun kokonais-valtaisessa muuttamisessa, tasapainoisen synergisen kokonaisuuden rakentamisessa ja vanhasta luopumisessa. Kaikki vaikeita ja isoja asioita.

UUSI VERKOSTOTEORIAN PARADIGMA: SKAALAVAPAA VERKKO

1. SKAALAVAPAA VERKKO: 2002

Uudenlaista ymmärtämistä verkostojen perusluonteeseen tarjoaa vuonna 2002 julkaistu verkostoteorian uuden paradigman muodostumista kertova kirja:"Linked; The New Science of Network".[71]

Kirjan mukaan verkostojen teorian historia ulottuu matemaatikko Leonhard Euleriin 1700- luvulle (graph theory). Viime vuosina (1999 - 2002) syntyneen uuden teorian sovellutuksia löytyi matematiikasta, fysiikasta, sosiologiasta, taloustieteestä, biologiasta, epidemiologiasta, kielitieteestä, tieteellisestä kirjoittamisesta, sodankäynnistä, terrorismista, ym.

Aiempi, noin 300 vuotta vallinnut tiede, asian hajottaminen pienempiin osiinsa ja näiden pienempien osien ymmärtäminen, on johtanut umpikujaan. Osoittautui, että osista kokonaisuuden rakentaminen voi tapahtua monella, lukemattomilla tavoilla, joista luonto käyttää vain muutamaa. Luonto siis kokeilee kaikkea ja valitsee elinkelpoisimmat.

Tullaan ensin kompleksisuuden hallintaan, seuraavien vuosisatojen tieteen pääteemaan. Toiseksi tullaan edellä mainitun kokeilemisen oleellisuuteen evoluutiossa. Periaate toimii jo mm. ohjelmistojen, algoritmien kehittämisessä, taloudessa, riskirahoituksessa ja sodankäynnissä.[72] Kyse on siis kaiken tieteen muuttumisesta osien tutkimisesta kokonaisuuksien tutkimiseen.

Vuonna 1959 Erdos'in ja Renyi'in keksimä vanha verkostoteoria perustui satunnaiseen verkkoon. Siinä oleellista olivat topologia, staattisuus ja satunnaisuus. Sen mukaan verkko oli valmiiksi olemassa ja yhteydet ja solmut olivat satunnaisia. Tästä seurasi mm. se, että solmujen yhteysmäärät olivat tilastollisesti jakautuneita (Poisson). Verkosta löytyi mm. tyypillinen solmu.

Uuden verkostoteorian mukaan verkot elävät ja kehittyvät eivätkä solmut ole tasa-arvoisia. Niiden kehitystä ohjaa keskeisesti (1) kasvu ja (2) houkuttelevuustekijä. Syntyy skaalavapaa malli. Sen solmujen yhteydet muodostava potenssi- (power) lain mukaisen jakautuman. Siinä ei ole tyypillistä solmua. Skaalavapaan mallin oleellisia ominaisuuksia ovat ensin siis kasvu ja houkuttelevuustekijä. Lisäksi niitä luonnehtii (3) hubit, kytkijät (hubs), eli hyvin runsaiden yhteysmäärien solmut. Kytkijät ovat todellisten verkkojen avaintekijät.

Verkon topologian kuvaamisesta ollaan siirrytty sen mekanismin ymmärtämiseen, joka muodostaa verkon dynamiikan. Muodostuu vastaparit staattinen - kasvava, satunnainen - skaalavapaa ja struktuuri - evoluutio

Todelliset verkot ovat hyvin yleisiä maailmassa, monella tieteenalalla. Verkkojen muodostuminen liittyy muodonmuutokseen. Todelliset verkot sisältävät useimmiten seuraavan suurrakenteen: Ensin on pienen lähipiirin voimakkaat ja kaikkia koskevat liitynnät, aliverkko, klusteri. Sitten muodostuu heikot yhteyden muihin klustereihin. Jo keskimäärin noin yhdellä yhteydellä per klusteri, aliverkot verkottuvat superverkoksi, joka alkaa elämään omaa elämäänsä. Heikot yhteydet ovat hyvin tärkeitä. Ensin ne muodostavat superverkon, vähillä yhteyksillä. Toiseksi niiden antama tieto on poikkeavaa klusterin homogeenisesta tiedosta.

Superverkosta tullaan aivan keskeiseen asiaan, emergenssiin.73 Sillä tarkoitetaan vaikeasti selitettävän ylätason käyttäytymisen syntymistä lukuisista alatason verkottuneista klustereista. Emergenssi on alhaalta ylös ilmiö. Emergenssi syntyy siis kun suuri määrä yksinkertaisia, verkottuneita ilmiöitä (klustereita) vaikuttaa yhdessä. Esimerkiksi tuhannet, kymmenet tuhannet muurahaiset. Tai ihmisen aivojen kaksi miljoonaa suuraluetta, neuroniklusteria. Alatason verkottuneet, yksinkertaiset ilmiöt luovat ylemmän, uuden, kompleksisen, adaptiivisen, itseorganisoituneen tason olemassaoloon: muurahaispesän makrokäyttäytyminen, ihmisen tietoisuus. Sillä on omat sääntönsä, jotka on hyvin vaikea johtaa se synnyttäneistä alemman tason yksinkertaisista ilmiöstä. Voidaan esim. ajatella, että tietoisuus on monimutkaisten aivojen 10 miljardin neuronin x- tasolle synnyttämä uusi olemassaolon ilmiö. Emergenssi on lukumääräsensitiivinen ilmiö. Alatason klustereita tarvitaan paljon (satoja?). Uutta tasoa voidaan käsitellä omanaan, ilman alemman tason ymmärtämistä. Uudella tasolla on täysin omat sääntönsä, vertaa esimerkiksi muurahaispesä käyttäytyminen tai ihmisen tietoisuus.

Jos edellä mainittu tasoilmiö on yleinen, kuten ilmeisesti on, tullaan mielenkiintoisiin johtopäätöksiin. Olemassaolo (Luonto) pyrkii siis uusille, korkeammille tasoille. Onko kaikkien asioiden ymmärtämisessä olemassa kyseinen tasoperiaate? Mitkä ovat asioiden, esim. sodankäynnin tasot tässä mielessä? Internet täyttää monet alatason ilmiön vaatimukset. Mikä on sen makrotaso? Mediassa on alkanut näkyä vuoden 1980- jälkeen uusia ilmiöitä. Media on verkottunut, sirpaloitunut (paljon elementtejä, klustereita) viime vuosikymmeninä. Selittääkö emergenssi media uudet ilmiöt. Mitä ilmeisemmin. Siis ne jotka johtuvat kyseistä dynamiikasta.

Klustereiden sovellutuksia löytyy mm. sosiologiasta, taloudesta, aivoista, biologiasta, fysiikasta ja sodankäynnistä. Sosiologiasta esimerkkejä ovat läheiset ystävät, taloudesta keiretsu- idea Japanin taloudessa, aivoista aivojen noin kaksi miljoonaa suuraluetta ja biologiasta läheiset solut, jotka kommunikoivat kemiallisesti keskenään. DNA:n lisäksi olion kehityksen vaikuttaa siis paikallinen informaatio, solujen kemian yhteen sitoma verkko. Edelleen fysiikasta esimerkkejä ovat jäätyminen ja magneetin muodostuminen. Ensin muodostuu useita atomeja käsittäviä, samalla tavalla "käyttäytyviä" atomiklustereita. Sodankäynnissä prikaatia voidaan pitää noin 1000 klusterina, eli ryhmänä, toimistona, ajoneuvokuntana tai vastaavana. Klusterit on tosin prikaatissa organisoitu yhteen enimmäkseen hierarkkisesti. Sen sijaan huomion arvoista on, että klusterit (ryhmät) ovat sodankäynnissäkin sisäisesti enimmäkseen täysin kytkettyjä verkkoja.

Klusterit ja niistä muodostuva superverkko on globaali/paikallinen- sovellutus. Miksi kyseinen rakenne näkyy niin monessa nykyajan ilmiössä? Klusterien ymmärtäminen on tärkeää monen ilmiön ymmärtämiseksi verrattuna yksittäisen toimijan ymmärtämiseen. Esimerkiksi atomiklusterit ovat aineen käyttäytymisessä tärkeämpiä kuin yksittäiset atomit.

80/20- sääntö liittyy usein suurimpiin klustereihin, eli kytkijöihin (hubs). Siis siihen, että toiminnassa on muutama avaintekijä, jotka vaikuttavat keskeisesti lopputulokseen. Keskittymällä avaintekijöihin, saadaan eniten tuloksia vähimmillä resursseilla.

On kuitenkin olemassa vielä tehokkaampi sääntö. Jo piirretään 80/20 säännön kuvaaja, joka siis kulkee pisteiden 0:0, 80:20 ja 100:100 kautta, havaitaan, että kyseinen käyrä kulkee myös noin pisteen 65:10 kautta. Siis puolittamalla vielä 80/20- säännön mukaiset panokset (20 –> 10), eli pudottamalla panoksia 50 prosenttia, tehokkuus laskee vain noin 19 prosenttia (80 –> 65). Seuraava panosten puolitus (10 –> 5) pudottaa tehokkuuden 65:stä 40:een. Puolet tuloksista saadaan noin kuuden prosentin panoksilla. Sotilaalliset sovellutukset klustereista ja 80/20 säännöstä ovat selviä: Vaikuttamalla pieneen osaan, erityisesti valittuihin klustereista, vaikutetaan merkittävästi koko verkkoon, eli prikaatiin. Klustereiden ymmärtäminen on siis tärkeää niille, joilla ei ole rajattomasti resursseja kaiken tuhoamiseen.

Verkko on hyvin kompleksinen rakenne. Verkko on siis merkittävä osa kompleksisuuden ymmärtämistä. Seuraava suuri haaste, seuraava tieteen vuosisata, on nimenomaan kompleksisuuden hallintaa. Tämä viittaa vahvasti fyysikko Heinz Pagelsiin vuodelta 1989. Pagelsin mukaan kompleksisuus on seuraavan 300 vuoden tieteen uusi teema. Kun edelliset kolme vuosisataa selvittiin kaukoputkella ja mikroskoopilla, seuraavat kolme vuosisataa keskeisenä tutkimusvälineenä, kompleksisuuden hallinnan välineenä, käytetään tietokonetta.[74]

2. UUDEN VERKOSTOTEORIAN HERÄTTÄMIÄ AJATUKSIA

Verkosta oli tullut ase, miekka. Tätä osoittavat uudet hajautetut palveluksenestohyökkäykset (DDoS), jossa hakkeri on saanut haltuunsa esimerkiksi sata tietokonetta verkossa ja laittaa ne hyökkäämään kohdetta vastaan koordinoidusti. Mielenkiintoista on myös F-Secure:n noin 2 tunnin vasteaika uusiin viruksiin. Ainoa järkevä tapa jakaa kyseinen tieto on verkko. Verkko siis toimii ainoastaan, jos verkko toimii?! Verkosta on siis tullut myös suoja, kilpi. Eli: Verkko on väline tehdä jotain kolmella tavalla: (1) toimintana (bisnes, posti, tiedonvälitys, prosessori-kapasiteetti...), (2) miekkana (hyökkäys) ja (3) kilpenä (puolustus). Verkko on hyökkäyksen väline ja suojauksen kohde. Tämä on sodankäynnin yleistä dynamiikkaa. Kun jokin asia tulee sodankäynnissä tärkeäksi, siitä tulee ensin hyökkäyksen ja sitten puolustuksen kohde. Vertaa esimerkiksi lentokone, tieto, radio, tutka.

Verkko on myös (super-)tietokone. Ensin nykyaikainen supertietokone on massiivinen rinnakkaistietokone. Siinä maksimissaan noin 10.000 nykyajan tehokkainta prosessoria toimii yhteen. Toiseksi tavallisesta koti- tai työtietokoneen prosessorikapasiteetista on vapaana noin 80 prosenttia. Kolmanneksi: Jos oletetaan, että Suomessa on noin 2.000.000 tietokonetta saadaan havainto, että Suomessa voisi olla käytössä noin 160 supertietokoneen kapasiteetti johonkin käyttöön, esimerkiksi tieteelliseen laskentaan tai salakirjoituksen murtamiseen. Tällä tavalla tulkittuna verkko on supertietokoneen supertietokone. Toki edellä mainitun potentiaalin muuttaminen todellisuudeksi vaatii vielä muutamaa asiaa verkon ja tietokoneiden lisäksi.

Yllä oleva esimerkki on myös valaiseva siinä mielessä, että näkemällä kyseiset resurssit

verkkona ja saamalla ne toimimaan verkkona, voidaan päästä merkittävään tehon säästöön ja taloudellisuuteen. Noin kahden miljardin euron taloudellisesta panoksesta on 80 prosenttia vapaana.

Ihmiskunnassa kaksi satunnaista ihmistä on keskimäärin kuuden linkin päässä toisistaan. Tämä on kokeellinen tieteellinen havainto vuodelta 1967. Pohjana tälle on se, että yksi ihminen tuntee noin 100 - 200 muuta ihmistä. Yksi linkki on siis 100 ihmistä, kaksi 10.000 ja kuusi linkkiä miljoona miljoona ihmistä, jos kyseiset ihmiset eivät tunne seuraavissa portaissa samoja ihmisiä.

Maailma on kutistumassa, koska ihmisten väliset yhteydet, jotka muutama vuosisata sitten olisivat kuolleet pitkiin etäisyyksiin, pysyvät hengissä nykyaikaisilla tietoliikenne ja liikenneyhteyksillä. Myös ihmisten kyky ylläpitää yhteyksiä on kasvanut samoista syistä radikaalisti. On puhuttu kuudesta, neljästä yhteydestä. Nykyään saatetaan olla jo lähellä kolmea. Tämä on todella merkittävä asia, kun kyseinen kehitys vaikuttaa muutamia vuosikymmeniä. Johtaako tämä maailmankulttuuriin, sodankäynnin vaikeuteen, ja niin edelleen? Onko globaali jatkossa oleellinen? Miksi globaali olisi jatkossa oleellinen? Globaali tietotekniikka voidaan myydä kerran yhtenä kappaleena tehtynä helposti (internetin välityksellä) koko globukselle. Aika ja etäisyys ei rajoita sen myyntiä. Myyntiä rajoittaa suljetut alueet (vapaa kauppa!), kulttuuriin sovittaminen (kulttuurituntemus!) ja infrastruktuurin puute (internet, tietokoneet!).

Koehavainto: Ihmisverkoissa löytyi yksilöitä, joilla oli paljon enemmän yhteyksiä, kuin satunnaisten verkkojen teoria salli. He olivat ympäristönsä supervaikuttajia, henkilöitä, jotka tunsivat kaikki ja jotka kaikki tunsivat. He luovat trendejä ja muotia. Kytkimiä (hubs) (kytkijöitä) löytyy monelta alalta, muualtakin kuin ihmisyhteisöistä. Webissä kyseisen tyyppiset kytkimet ovat verkon avaimia. Kytkijöitä ei pitäisi olla olemassa satunnaisten verkkojen teoriassa. Kytkijöiden houkuttelevuuteen katoaa webin näennäinen demokraattisuus: Kuka tahansa voi julkaista mitä tahansa kaikille webissä. Tämä pitää paikkansa. Sen sijaan se mitä luetaan on aivan eri asia. Webissä on oleellista, montako sisään tulevaa linkkiä dokumentilla on.

Kompleksisten verkkojen ominaisuus on se, että liitettävyydestä johtuu haavoittuvuutta. Tästä puhutaan verkkosodan tutkimuksen yhteydessä.

Internet on verkkojen verkko. Sen ymmärtäminen ei ole matemaattinen tai insinöörion-gelma. Internet on enemmän ekosysteemi kuin kello. Se ei ole keskitetysti suunniteltu. Internet on aivan oleellinen jatkossa. Se on selvästi kompleksinen, verkottunut järjestelmä, joka muodostaa ylätason uutta toimintaa. Internet on piihin perustava, rinnakkainen universumi hiileen ja elämään perustuvaan tavalliseen universumiin verrattuna. Onko internet uudenlaisen teknisen evoluution alusta, infrastruktuuri?

Vuonna 2010 maailmassa on noin 10.000 telemetristä laitetta jokaista ihmistä kohti, x miljardia kännykkää, y miljardia tietokonetta. Ja kaikki samassa verkossa. Kun tähän vielä lisätään ohjelmistojen älykkyyden lisääntyminen, adaptiiviset ohjelmat ja henkilökohtaiset agentit, saadaan näkemys, että internet on jatkossa aivan oleellinen, emmekä tiedä mihin emergentteihin ilmiöihin se johtaa. Niin paitsi Stanislaw Lem tietää kirjassaan "Kyberias".

Sodankäynnissä vaikuttaa keskeinen verkostojen ominaisuus, rekursiivinen, itseensä viittaava järjestelmä. Rekursiivista viittauksesta syntyy usein epälineaarinen vaikutus. Sodankäynnin ydin, kaksintaistelu, on rekursiivinen, itseensä viittaava järjestelmä: Vaikutan viholliseen, jolloin sen vaikutus minuun vähenee, jolloin minun vaikutus viholliseen kasvaa, jolloin... Seuraa Lancasterin yhtälöt, jossa oman lukumääräisen ylivoiman vaikutus vastustajan tappioihin on toiseen potenssiin verrannollinen, siis potenssiin liittyvä, siis epälineaarinen.

Entä terrorismi? Kyse on useimmiten nimenomaan pienistä soluista (klusterit yllä!), jotka yhdistyvät kokonaisuudeksi, superstruktuuriksi hyvin vähillä yhteyksillä per solu. Noin yksi yhteys per solu riittää verkon, ylätason vaikutuksen muodostumiseen! Useampi yhteys taas olisikin jo riskitekijä.

[1] Suomennoksissa on lähdetty linjasta war = sota ja warfare = sodankäynti sekä net = verkko ja network = verkosto. Poikkeus on computer network, joka edellisen linjan mukaan olisi tietokoneverkosto. Verkosto viittaa suomen kielessä kuitenkin ennen kaikkea ei-tekniseen (ihmissuhdeverkosto, ei ihmissuhdeverkko, kalaverkko, ei kalaverkosto (tai se ei ainakaan tarkoittaisi kalojen pyytämiseen tarkoitettua teknistä rakennetta)). Computer network on siis käännetty tietokoneverkko.

[2] Netwar on käännetty tekstissä verkkosodaksi. Vastaavasti Network-Centric Warfare (NCW) on käännetty verkostokeskeiseksi sodankäynniksi.

[3] Ensimmäinen merkkipaalu: Arquilla, John, and David Ronfeldt:"Cyberwar is coming!" Comparative Strategy, Volume 12, Kevät 1993, no. 2, s. 141-165
Toinen: A. K. Cebrowski, J. J. Garstka:"Network-Centric Warfare; Its Orgin ja Future", Proceedings January 1998 s. 28 - 35.
Kolmas: (a) Z P Hubbard:"Information Warfare in Kosovo" Journal of Electronic Defence November 1999 s. 57 - 60
(b) Journal of Electronic Defence, January 2000 s. 13: US Army Research Laboratory:n ilmoitus: Information Operation Conference February 8. - 9. 2000" Session Two:"Normalization Computer Network Attack (CNA) as a Legitime Tool of War. CNA- istunto oli "Salainen , vain USA:n kansalaisille" ("Secret, U.S. Only"). Ko. CNA- istunnon osia olivat:
- U.S. Computer Network Attack Programs
- The Role of IO (Information Operations) in Coalition Operations
- International Arms Control Regimes
- Status of International Discussions
- Legal Issues in CNA
(C) USA on muodostanut uuden Hyökkäyksellisen Informaatiosodankäynnin johtoportaan (Offensive Information Warfare Command) 1.10.2000. Sen pohjana on US Space Command ja Defence Information System Agency:n The Joint Task Force Computer Network
Neljäs: USA:n puolustusministeriön raportti "Network-Centric Warfare" USA:n kongressille 27.7.2001 (http://www.dodccrp.org/NCW/NCW-report/report/ncw-cover.html 5.1.2003) ja
Viides: Albert-Laszlo Barabasi:"Linked; The New Science of Network" Persus Publishing USA 2002

[4] Hierarkiakin on yksi verkkomuoto, eli puu tai pyramidi. Muita verkkomuotoja ovat linja, ympyrä, hila, täysin kytketty verkko ja näiden erilaiset yhdistelmät. Täysin kytketty verkko tarkoittaa rakennetta, jossa jokaiseen solmuun on suora yhteys jokaisesta muusta solmusta.

[5] John Arquillan haastattelu Telepolis - lehdessä 13.3.2001 (Stefan Krempl). Haastattelussa Arquilla kertoo, että Kosovossa oli toiminnassa lukuisia USA:n erikoisjoukkojen ryhmiä yhteistyössä KLA:n kanssa. Ne hiillostivat serbien joukkoja piilopaikoistaan. (http://www.heise.de/tp/english/inhalt/te/7122/1.html 3.1.2003)

[6] (a) Z P Hubbard:"Information Warfare in Kosovo" Journal of Electronic Defence November 1999 s. 57 - 60
(b) Journal of Electronic Defence, January 2000 s. 13: US Army Research Laboratory:n ilmoitus: Information Operation Conference February 8. - 9. 2000" Session Two:"Normalization Computer Network Attack (CNA) as a Legitime Tool of War. CNA- istunto oli "Salainen , vain USA:n kansalaisille" ("Secret, U.S. Only"). Ko.

CNA- istunnon osia olivat:
- U.S. Computer Network Attack Programs
- The Role of IO (Information Operations) in Coalition Operations
- International Arms Control Regimes
- Status of International Discussions
- Legal Issues in CNA

(C) USA on muodostanut uuden Hyökkäyksellisen Informaatiosodankäynnin johtoportaan (Offensive Information Warfare Command) 1.10.2000. Sen pohjana on US Space Command ja Defence Information System Agency:n The Joint Task Force Computer Network.

[7] (1) M Lubicki:"What is Information Warfare ?" National Defence University ACIS Paper 3 August 1995 Prefase (Internet http://www.ndu.edu/inss/actpubs/act003/a00ch00.hmtl 31.12.2002)
(2) S Ahvenainen:"Sodankäynnistä, elektroniikasta ja elsosta" Tiede ja Ase N:o 52/1994 s. 91 - 139, luku 1.6. Sodankäynnin yleiset ulottuvuudet (s. 98 - 101)

[8] M Lubicki:"What is Information Warfare ?" National Defence University ACIS Paper 3 August 1995 Prefase (Internet http://www.ndu/inss/actpubs/act003/a00ch00.hmtl 31.12.2002)

[9] PEjojä-os esittely R2805/12/E/IV Pv:n operaatiopäällikölle 27.9.2001:"Luonnoksena käyttöön otettavat informaatio- ja johtamissodankäynnin sekä elektronisen sodankäynnin määritelmät"

[10] M Libicki:"What Is Information Warfare ?" Chapter 6 s.1 - 4. (Internet: http://ndu.edu/inss /actpubs/act003/a003ch06.html 31.12.2002)

[11] Näiden osalta ks alkuperäinen lähde (Libicki)

[12] Tämä luku (1.2) perustuu tietoulottuvuutta lukuun ottamatta tutkimukseen S Ahvenainen:"Sodankäynnistä, elektroniikasta ja elsosta" Tiede ja Ase N:o 52/1994 s. 91 - 139, luku 1.6. Sodankäynnin yleiset ulottuvuudet (s. 98 - 101)

[13] M Howard:"The Forgotten Dimensions of Strategy" Foreign Affairs Summer 1979 s.976- 7

[14] C von Clausewitz:"On war" Princeton University Press 1976 s.136

[15] G I Seffers:"Survey: Software Costs To Exeed Hardware" Defence News November 10-16, 1997 s. 6

[16] H Sokala:"Uutiset" Helsingin Sanomat 18.6.1999 s. D 1

[17] Salamasodan analyysi perustuu pääosin OODA- loop'n keksijän John Boyd'n esitykseen "Pattern of Conflict" Joulukuu 1986 s.66 - 89

[18] M van Creveld:"Suppling War; Logistics from Wallenstein to Patton" Cambridge University Press, Campridge 1977. Luku 5:"Russian Rulette" s. 142 - 180. Logistiikan puolella menestys Venäjällä oli Creveldin mukaan enemmänkin organisaatiotaidossa ja johtajien antamisessa kaikkensa ongelmien ratkaisemiseen kuin logistisen järjestelmän erinomaisuudessa.

[19] USA:n Puolustusministeriön raportti "Network Centric Warfare" 27.7.2001 USA:n kongressille s. 3-8 - 3-11. Varsinaista "selvää" määritelmää VKS:lle ko. raportissa ei esitetä.
(http://www.dodccrp.org/NCW/NCW-report/report/ncw-cover.html 5.1.2003)

[20] http://www.informatik.umu.se/~rwhit/IWGlossary.html 31.12.2002

[21] Rona, Thomas P:"Weapon systems and information war" Seattle: Boeing Aerospace Co. research report, July 1976.

[22] Campen, Alan D:"Rush to information-based warfare gambles with national security" SIGNAL, Vol. 49, no. 11 (July 1995), pp. 67-69.

[23] USA:n puolustusministeriön sotilaalliset termit

[24] Widnall, Sheila E., and Gen. Ronald R. Fogleman:"Cornerstones of information warfare" s. 2 Washington D.C.: Dept. of the Air Force, October 1995.
http://www.af.mil/lib/corner.html 31.12.2002

[25] Stein, George J:"Information Warfare" s. 32 Airpower Journal , Spring 1995.
http://www.airpower.maxwell.af.mil/airchronicles/apj/stein.html 31.12.2002

[26] Szafranski, Richard (Col.):"A theory of information warfare: Preparing for 2020" Airpower Journal, Vol. IX, no. 1 (Spring 1995), s. 65. Alaviite 1
http://www.airpower.maxwell.af.mil/airchronicles/apj/szfran.html 31.12.2002

[27] Szafranski, Richard (Col.):"A theory of information warfare: Preparing for 2020" Airpower Journal, Vol. IX, no. 1 (Spring 1995), s. 58
http://www.airpower.maxwell.af.mil/airchronicles/apj/szfran.html 31.12.2002

[28] Tämän kappaleen määritelmät ovat Umeån yliopiston informaatiosodankäynnin tutkijan kotisivuaineistosta: http://www.informatik.umu.se/~rwhit/IWGlossary.html 31.12.2002

[29] US Army:n ohjesääntö 6.12.1995 FM 100-6 "Informations Operations" Headquarters, Departement of the Army, Washington DC, s. 2-2

Uusimmat määrittelyt liittävät informaatiosodankäyntiin tietokoneverkkohyökkäykset, CNA (Computer Net-

work Attack). Niiden osalta katso esim.: (a) Z P Hubbard:"Information Warfare in Kosovo" Journal of Electronic Defence November 1999 s. 57 - 60
(b) Journal of Electronic Defence, January 2000 s. 13: US Army Research Laboratory:n ilmoitus: Information Operation Conference February 8. - 9. 2000" Session Two:"Normalization Computer Network Attack (CNA) as a Legitime Tool of War. CNA- istunto oli "Salainen , vain USA:n kansalaisille" ("Secret, U.S. Only"). Ko. CNA- istunnon osia olivat:
- U.S. Computer Network Attack Programs
- The Role of IO (Information Operations) in Coalition Operations
- International Arms Control Regimes
- Status of International Discussions
- Legal Issues in CNA
(C) USA on muodostanut uuden Hyökkäyksellisen Informaatiosodankäynnin johtoportaan (Offensive Information Warfare Command) 1.10.2000. Sen pohjana on US Space Command ja Defence Information System Agency:n The Joint Task Force Computer Network.

[30] PEjojä-os esittely R2805/12/E/IV Pv:n operaatiopäällikölle 27.9.2001:"Luonnoksena käyttöön otettavat informaatio- ja johtamissodankäynnin sekä elektronisen sodankäynnin määritelmät"

[31] US DoD Military Definitions: Information warfare ja Information operations
http://www.dtic.mil/doctrine/jel/doddict/index.html 3.1.2003

[32] Thomas P. Rona:"Weapon systems and information war", tutkimusraportti, Seattle: Boeing Aerospace Co.Heinäkuu 1976

[33] Joint Pub 3-13.1 "Joint Doctrine for Command and Control Warfare" USA, 7.2.1996 s. GL 4 - 5

[34] PEjojä-os esittely R2805/12/E/IV Pv:n operaatiopäällikölle 27.9.2001:"Luonnoksena käyttöön otettavat informaatio- ja johtamissodankäynnin sekä elektronisen sodankäynnin määritelmät"

[35] US DoD Military Definitions: Command and Control Warfare (lyhennetty tähän)
http://www.dtic.mil/doctrine/jel/doddict/index.html 3.1.2003

[36] Esimerkiksi USA:n asevoimien Joint Pub 3-13.1 "Joint Doctrine for Command and Control Warfare (C2W)" 7.2.1996 korvaa teoksen Joint Pub 3-13 "C3CM in Joint military Operation" 10.9.1987 (Lähde USA:n asevoimien Joint Pub 3-13.1 "Joint Doctrine for Command and Control Warfare (C2W)" 7.2.1996,. Appendix D: "Admistrative Instructions" s. D-1

[37] RAND Corporation:"The fly on the wall and the Jedi Knight" Research Brief (abstract) for Hundley, Richard O,. and Eugene C. Gritton, Future Technology-Driven Revolutions in Military Operations: Results of a Workshop, RAND Report DB-110-ARPA, 1995. http://www.rand.org:/publications/RB/RB7104/RB7104.html 31.12.2002

[38] Campen, Alan D:"Vulnerability of Info Systems Demands Immediate Action: Reliance by Military on Commercial Communications Infrastructure Poses Significant Peril to United States" National Defense , November 1995

[39] AFCERT AFCERT Computer Glossary, cyberspace

[40] Tämän kappaleen määritelmät ovat Umeån yliopiston informaatiosodankäynnin tutkijan kotisivuaineistosta: http://www.informatik.umu.se/~rwhit/IWGlossary.html 31.12.2002

[41] Microsoft Bookself 99, hakusana "cyberspace", sanakirjaosuus (Chambers Dictionary). Ko. sanakirjassa ei löydy sanaa cyberwar.

[42] Cyberspace, environment created by the global networking of computer systems. The term is widely applied to the Internet as it exists today, but in its origins in science fiction it referred to a far more ambitious and speculative conception: the total immersion of the human senses in an artificially generated environment. The human being's sensory experience would actually be generated by the machine and fed directly into the human brain.
The term "cyberspace" was popularized by the science-fiction author William Gibson in his book Neuromancer. In this, cyberspace is defined on a children's show, itself in cyberspace, as:
... A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts ... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding ...
The other aspect of cyberspace is indicated by this quotation: as a system for organizing and accessing the vast amounts of data stored on computers. Currently the Internet, and especially that facet of it called the World Wide Web, is the major system for collating and accessing the huge store of electronic data. The Web is vastly superior to any system before it, but it is still rather limited. Interaction with the Web is slow. The data can only be searched sequentially. There is no way of grouping information about similar topics apart from links that can be incomplete or inaccurate. Within true cyberspace not only would the data be represented

in a three-dimensional visual form, but the user could interact with the objects verbally or even physically. Whereas virtual reality is the fooling of the senses so that the person believes he or she is in a different environment, true cyberspace would involve a complete integration of the person with the machine. (Lähde: Microsoft Encarta 99 Encyclopedia Deluxe Version, artikkeli:"Cyberspace".

[43] US DoD Military Definitions: Cyberspace
http://www.dtic.mil/doctrine/jel/doddict/index.html 3.1.2003

[44] Grier, Peter:"Information Warfare" Air Force Magazine, March 1995 s. 37

[45] Szafranski, Richard (Col.):"A theory of information warfare: Preparing for 2020" s. 58 Airpower Journal, Vol. IX, no. 1 (Spring 1995)
http://www.airpower.maxwell.af.mil/airchronicles/apj/szfran.html 31.12.2002

[46] Libicki, Martin C:"What is information warfare?" National Defense University Strategic Forum Report Number 28, May 1995.

[47] Arquilla, John, and David Ronfeldt:"Cyberwar is coming!" Comparative Strategy, Volume 12 (1993), no. 2, s. 141-165

[48] Arnett, Eric H:"Welcome to hyperwar" The Bulletin of the Atomic Scientists, Vol. 48, No. 7, September 1992, s. 14-21.

[49] Älykkäiden koneiden ja järjestelmien toiminta pohjautuu ihmisen määrittämiin sääntöihin, virtuaalisiin geeneihin, algoritmeihin, ohjelmistoissa. Jos koneet kehittyvät tietoisiksi teknisessä evoluutiossa, kuten ihminen biologisessa evoluutiossa, ne ymmärtävät lopulta toimintansa pohjana olevan virtuaalisen geenistön ja pystyvät sitä kautta irtautumaan sen vaikutuksesta. Tämän perusteella ihmisillä on ote koneisiin niin kauan, kun ne ovat koneita, eli eivät ole tietoisia itsestään. Tullessaan tietoisiksi itsestään, ne muuttuvat elektronisiksi tietoisiksi olioiksi, kun ihminen on biologinen tietoinen olio.
Tämän muutoksen eroista todettakoon, että ihmisen biologis- kemialliset hermoimpulssit kulkevat noin nopeudella 3 - 300 km/h. Vastaavasti elektroninen signaali kulkee valon nopeudella, 300 - 3 miljoonaa kertaa nopeammin! Eli kun ihmisen aivojen koko, suurin etäisyys (20 cm) edellä mainitulla suurimmalla nopeudella vastaa kahta millisekuntia, voi elektroniset aivot olla suurimmalta etäisyydeltään 600 kilometriä. Edelleen tämän tulkinnan mukaan eläimet, jotka eivät ole tietoisia itsestään ja itseään ohjaavista geeneistä, ovat biologisia koneita. Tämä tietoisuuteen ja ymmärtämiseen liittyvä näkökulma viittaa vahvasti 1600- luvun filosofi Benedict Spinozaan. Hän sanoi, että ymmärtäminen on tie eteenpäin, tie vapautumiseen pahasta (Ahvenainen: Siis geenien tai koodien merkityksestä). (Spinoza (1677): "Ethics". Wordsworth Edition Limited, Englanti (2001) s. LXVIII, LXXVIII, P5P3)

[50] Libicki, Martin C:"What is information warfare?" National Defense University Strategic Forum Report Number 28, May 1995.

[51] Szafranski, Richard (Col.):"A theory of information warfare: Preparing for 2020" s. 58 Airpower Journal, Vol. IX, no. 1 (Spring 1995)
http://www.airpower.maxwell.af.mil/airchronicles/apj/szfran.html 31.12.2002

[52] Arquilla, John, and David Ronfeldt:"Cyberwar is coming!" Comparative Strategy, Volume 12 (1993), no. 2, s. 141-165

[53] A Campen:"Promise and peril of Information-Based Warfare" InfoWarCon95 Proceedings s.L5. Alunperin Arquilla & Ronfied:"Cyberwar is comming!" Comparative Strategy Volume 12 No 2 sivut 141 - 165 (kappale: "Explaining Netwar")

[54] D S Albert & J J Garstka & F P Stein:"Network Centric Warfare; Developing and Leveraging Information Superiority" CCPR 1999 s.2

[55] USA:n Puolustusministeriön raportti "Network Centric Warfare" 27.7.2001 USA:n kongressille s. 3-8 - 3-11. Varsinaista "selvää" määritelmää VKS:lle ko. raportissa ei esitetä.
(http://www.dodccrp.org/NCW/NCW-report/report/ncw-cover.html 5.1.2003)

[56] Lain kritiikistä ks T Paukku:"Mooren laki - teknologian väärä hokema" Helsingin Sanomat 4.1.2003 s. C 13, joka perustuu tutkija Ilkka Tuomen 30- sivuiseen esitykseen. Tosiasia on kuitenkin yhden mikropiirin (mikroprosessorin) transistorien määrän jatkuva kasvu ja kellotaajuuden jatkuva nopeutuminen. Ensimmäinen mikroprosessori Intel 4004 vuodelta 1971 sisälsi muutamia tuhansia transistoreja ja sen kellotaajuus oli 100 kHz. Viimeisimmät mikroprosessorit (Pentium IV) sisältävät kymmeniä miljoonia transistoreja ja niiden kellotaajuudet liikkuvat muutamissa gigahertzeissä. Yksinkertaistettuna nämä luvut merkitsevät noin 10.000 * 10.000 = sata miljoonakertaista (transistorimäärä * nopeus)- tekijän kasvua. kolmenkymmenen vuoden ajalla. Säännöllisenä vuosikasvuna tämä merkitsee noin 85 prosentin kasvua joka vuosi.

[57] Tieteen Kuvalehden 3/99 ja Kompuutteri kaikille- lehden 3/99 yhteisliite s.2. Mikroprosessoreita oli siis vuonna 1999 valmistettu noin 15.000 miljoonaa.

[58] M Wilenius:"Informaatio marssii esiin" Helsingin Sanomat 31.1.1998 s.C 2 (Alunperin M Castells:"The Information Age; Economy, Society and Culture" Volume III s.356 - 360)

[59] KTT Jaarnila:"Ylen Avoin Yliopisto" Suomen TV 1 sunnuntaina 23.5.1999 klo 11.00 - 12.00

60 M Castells:"The Information Age: Economy, Society, And Culture" Volume I "The Rise of The Network Society" Blackwell Publishers Inc. USA 1999 s. 477

[61] Esimerkiksi yksinkertaisessa kolmitasoisessa hierarkkisessa organisaatiossa, esimerkiksi pataljoonassa, jossa on aina kolme alaista alaspäin saadaan seuraava rakenne: Yksi pataljoonan komentaja, kolme komppanian päällikköä ja yhdeksän joukkueen johtajaa. Yhteensä 13 toimijaa ja 12 kaksisuuntaista yhteyttä (9 * (kpääll - jjoht) + 3 * (pkom - kpäälll)). Jos edellä mainitut toimijat organisoidaan täysin kytkettyyn verkkoon, jossa jokaisella on yhteys jokaiseen, syntyy organisaatio, jossa on 13 toimijaa ja 156 kaksisuuntaista yhteyttä (13*12).

[62] Comparative Strategy Volume 12 (1993) No 2 sivut 141 - 165 (kappale:"Explaining Netwar")

[63] A Campen:"Promise and peril of Information- Based Warfare" InfoWarCon95 Proceedings s.L5. Alunperin Arquilla & Ronfied:"Cyberwar is comming!" Comparative Strategy Volume 12 No 2 sivut 141 - 165 (kappale: "Explaining Netwar")

[64] USS Shark 17.5.1987: Yksinäinen laivasto ja etenkin yksinäinen laiva oli todettu haavoittuvaksi ilmauhkaa vastaa. Em tapahtumasta alkoi US Navy:n verkkokeskeinen sodankäynti ja sen kulmakiven Cooperative Engagement Capability:n, CEC:n luominen (Lähde: B P Rivers & M Puttre:"Victory at CEC; US Navy presents its battle plan for network-centric warfare" Journal of Electronic Defence September 2001 s. 40)

[65] Proceedings January 1998 s. 28 - 35.

[66] Ks esim. USA:n Puolustusministeriön raportti "Network Centric Warfare" 27.7.2001 USA:n kongressille s. 8-9 ... 8-36 (http://www.dodccrp.org/NCW/NCW-report/report/ncw-cover.html 5.1.2003)

[67] Albert-Laszlo Barabasi:"Linked; The New Science of Network" Persus Publishing USA 2002

[68] Katso tarkemmin: S Johnson"Emergence; The connected life of ants, brains, cities and software"Scribner 2001 USA

[69] H Pagels:"The Dreams of Reason; The Computer and the Rise of Sciences of Complexity" Bantam Books 1989 USA

[70] Laajemmalle yleisölle termi esiteltiin vasta 1998 Proceedings of the Naval Institute- lehdessä Tammikuu 1998 s. 28 - 35. (Lähde: USA:n Puolustusministeriön raportti "Network Centric Warfare" 27.7.2001 USA:n kongressille s. 3-2; http://www.dodccrp.org/NCW/NCW-report/report/ncw-cover.html 5.1.2003)

[71] Albert-Laszlo Barabasi:"Linked; The New Science of Network" Persus Publishing USA 2002

[72] (1) Ohjelmistojen ja algoritmien kokeilu: Aloitetaan jostakin ohjelmaversiosta, luodaan siihen satunnaisvaihtelua ja testataan palautteen avulla saatuja ohjelmia halutun suorituskyvyn suhteen. (Katso tarkemmin: S Johnson"Emergence; The connected life of ants, brains, cities and software"Scribner 2001 USA)

(2) Talous: Japanilainen keiretsu- periaate. Siinä yhden pankin ympärille muodostunut yritysverkko, yritysklusteri, toimii uusien ideoiden, tuotteiden ja kokeilujen alustana. Vain osa tuotteista menestyy, mutta menestyneet tuotteet pitävät koko klusterin, eli pankin hengissä.

(3) Riskirahoitus: Vain osa, eli elinkelpoisimmat, rahoitettavista yrityksistä menestyy, mutta ne pitävät riskirahoitusfirmat pystyssä.

(4) Sodankäynti: Ensimmäisen maailmasodan saksalaisten itsenäiset iskuryhmät lähetettiin verkkona eteenpäin. Vain osa saavutti menestystä.

[73] Katso tarkemmin: S Johnson"Emergence; The connected life of ants, brains, cities and software"Scribner 2001 USA

[74] H Pagels:"The Dreams of Reason; The Computer and the Rise of Sciences of Complexity" Bantam Books 1989 USA

3. TIEDON MERKITYS SUOMEN PUOLUSTAMISESSA

Tuija Helokunnas, Terhi Laukkanen, Kalle Viitanen
Tampereen Teknillinen Yliopisto
Tiedonhallinnan laitos

3.1 Tiedon merkitys tavoitteellisessa toiminnassa

Puolustusvoimien määritelmäluonnoksen (27.9.2001) mukaan informaatiouhkat kohdistuvat tahtoon, tietoon ja tietojärjestelmiin pyrkien tahallisesti tai tahattomasti heikentämään tai kyseenalaistamaan näiden luottamuksellisuuden, eheyden tai saatavuuden tietoteknisillä, elektronisilla, fyysisillä tai psykologisilla menetelmillä. Tämän artikkelin tarkoituksena on kuvata tiedon ja osaamisen merkitystä tietoteknisten menetelmien avulla yhteiskuntaa vastaan kohdistuvilta informaatiouhkilta puolustauduttaessa.

Tiedolla on aina ollut keskeinen asema ihmisten toiminnassa. Tieto on toiminnan keskeisin elementti ja tietoon vaikuttamalla vaikutetaan kaikkeen toimintaan. Tiedon saatavuudella on kuitenkin eri toimijoille erilainen arvo eri ajankohtina. Tiedon arvo on siis määriteltävä kutakin tiedon suojaus- ja käyttötilannetta varten erikseen.

Ahvenainen (2002a) on John Boyd'n tunnettuun Object, Orient, Decide, Act (OODA)-silmukkaan (Hammond 2001) ja tekemisen edellytyksiin (Pöyhönen 1998) perustuen luokitellut toiminnassa tarvittavan tiedon seuraavasti:

1. Havainnointi: Tieto tekemisen tarpeesta
2. Perehtyminen: Tieto toiminnan kohteena olevasta kokonaisuudesta. Kokonaisuutta kuvaavan järjestelmäkäsityksen hahmottaminen perustuu geneettiseen perimään, kulttuuritraditioon, aiempiin kokemuksiin ja saatuun uuteen havainnointitietoon.
3. Päätös: Tieto siitä että mitä tekemisen tarpeen ja kokonaisuuden tuntien on järkevintä tehdä.
4. Toiminta: Tarvittavan asian tekemisessä välttämätön osaaminen, rohkeus, tahto ja kestävyys. Osaaminen perustuu tietoon joten osaamiseen sisältyy neljäs tavoitteellisessa toiminnassa tarvittavan tiedon luokka.

Alkuperäinen OODA-silmukka kuvaa johtamisessa tarvittavia tietoja. Ahvenaisen (2002a) luokittelu kattaa johtamisen lisäksi kaiken tavoitteellisen tekemisen. Ahvenaisen luokittelussa OODA-silmukkaa tulkitaan tiedon ja tekemisen näkökulmasta. Ahvenainen on erityisesti tuonut konkreettista sisältöä toiminta-kohtaan.

Esimerkiksi mikrotukihenkilölle saapunut ilmoitus maailmalla leviävästä viruksesta on tieto tekemisen tarpeesta. Mikrotukihenkilö perehtyy viruksesta annettuun tietoon ja havaitsee viruksen vaaralliseksi organisaatiolleen. Mikrotukihenkilö päättää lähettää vi-

ruksesta varoittavan sähköpostin kaikille organisaatiossa työskenteleville henkilöille sekä päättää päivittää käyttäjien saatavissa olevan virustorjuntaohjelmiston välittömästi. Mikrotukihenkilö päivittää virustorjuntaohjelmiston. Mikrotukihenkilö osaa päivittää virustorjuntaohjelmiston ja hänellä on rohkeutta tehdä päivitys: hän ei pelkää tuhoavansa muita ohjelmistoja tai tietoja tehdessään päivitystä. Mikrotukihenkilöllä on myös tahto tehdä päivitys: tahtoa saattaa heikentää esimerkiksi epävarma työllisyystilanne. Mikrotukihenkilöllä on päivityksen tekemiseen vaadittava kestävyys: työ ei jää kesken ja unohdu kun työkaveri pyytää mikrotukihenkilöä selvittämään toista ongelmaa. Lisäksi mikrotukihenkilö tarvitsee sekä havainnoimisessa, perehtymisessä, päätöksessä että toiminnassa resursseja kuten aikaa työn tekemiseen ja tarvittavat työvälineet.

Nykyisessä yhteiskunnassa tiedon merkitys on korostunut ja tieto on nostettu perinteisten tuotannontekijöiden rinnalle. Paitsi tuotannontekijä, on tieto itsessään myös tuote; useat tuotteet ja palvelut koostuvat suureksi osaksi datasta tai informaatiosta. Tiedon merkityksen korostumiseen on keskeisesti vaikuttanut tieto- ja viestintäteknologian (ICT, Information and Communication Technology) tarjoamien palveluiden nopea kehittyminen. Suomi on yhteiskuntana ollut edelläkävijä näiden teknologioiden kehittämisessä ja laajassa käyttöön ottamisessa. Teknologioiden kehittymiselle on ollut ominaista yhä nopeampi kasvu eli tuotekehityssyklit ovat nopeutuneet ja teknologioiden elinkaaret ovat lyhentyneet entisestään. Suomi 2015 –ohjelman (Sitra 2001) mukaan yksi Suomen strateginen tavoite on jatkossakin toimia suunnannäyttäjänä tieto- ja viestintäteknologiassa. Tulevaisuuden perustana on siis tieto- ja viestintäteknologian ja siihen liittyvän osaamisen laajentaminen kaikille toimialoille.

3.2 Tieto ja osaaminen

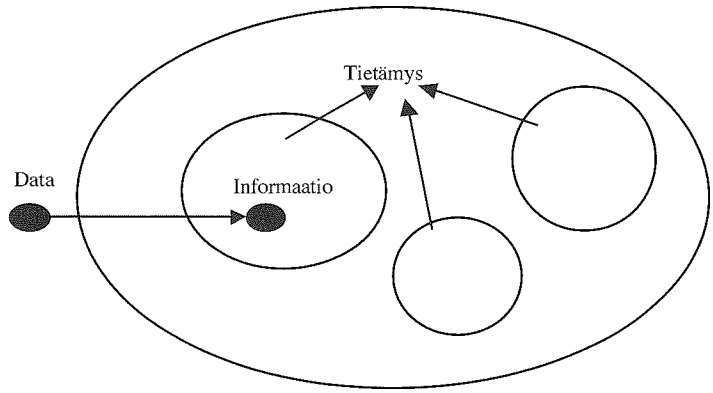
3.2.1 Tiedon hierarkkisuus ja laadullisuus

Tiedon hierarkkiset tasot ovat jalostumattomimmasta monimutkaisimpaan: data, informaatio ja tietämys. Data on mittaamalla tai havainnoimalla saatuja strukturoituja tuloksia (Davenport & Prusak 1998). Data määritellään myös aistihavainnoksi, kuten esimerkiksi ihmisen hermoa pitkin eteneväksi sähköimpulssiksi sekä merkkijonoksi, jota esimerkiksi tietokone käsittelee (Niiniluoto 1997). Data muuttuu informaatioksi asiayhteyteen liitettäessä, jolloin data saa havainnoijan ymmärtämän merkityksen. Informaatio taas muuttuu havainnoijan aivoissa tietämykseksi (knowledge), kun se ymmärretään laajemmin ja sitä voidaan hyödyntää esimerkiksi toiminnan pohjana (Kuva 2 ja 3).

Tiedon laji	Määritelmä	Prosessi
tietämys	analysointua, suhteutettua ja ymmärrettyä informaatiota	päättely perustelu epävarmuuksien hallinta
informaatio	data kiinnitettynä asiayhteyteen	järjestäminen sijoittaminen merkitysyhteyksiin yhdistely ristiriitaisuuksien poisto
Data	faktaa ilman asiayhteyttä	esikäsittely asettelu suodatus merkintä

Kuva 2 Tiedon hierarkkia, osit. (Waltz 1998), (Halonen 2000), (Thierauf 2001), Kuusisto (2002).

Tiedon hierarkkisen jaottelun soveltaminen tietoverkkoihin tuottaa seuraavan esimerkin: IP -osoite numeerisessa muodossaan on dataa kuten 102.21.200.111. IP-osoitteesta tulee informaatiota, kun tiedetään mitä toimintoja kyseisen IP -osoitteen omaavalla palvelimella suoritetaan kuten että palvelimella 102.21.200.111 sijaitsee tutkittavan valtion informaatiosodankäynnin virtuaaliopetusmateriaali. Tietämystä on edellisen tiedon yhdistämistä muuten saatuun tietoon, laajemman käsityksen luomista ja asiayhteyksien ymmärtämistä. Esimerkiksi kun tutkitaan virtualiopetusmateriaalin rakennetta ja painopistealueita sekä saadaan tietää, että materiaalin luonut valtio on myös julkaissut uuden informaatiosodankäynnin doktriinin, niin voidaan tehdä johtopäätös, että kyseinen valtio on siirtynyt sodankäynnissä uudelle tasolle, informaatiosodankäyntiin. Voidaan myös oivaltaa, että tämän uuden sodankäynnin ymmärtäminen on oman valtion puolustamisessa hyvin tärkeää.



Kuva 3 Data muuttuu informaatioksi kun se liitetään asiayhteyteen. Informaatio muuttuu tietämykseksi kun se analysoidaan, suhteutetaan ja ymmärretään (Kuusisto 2002).

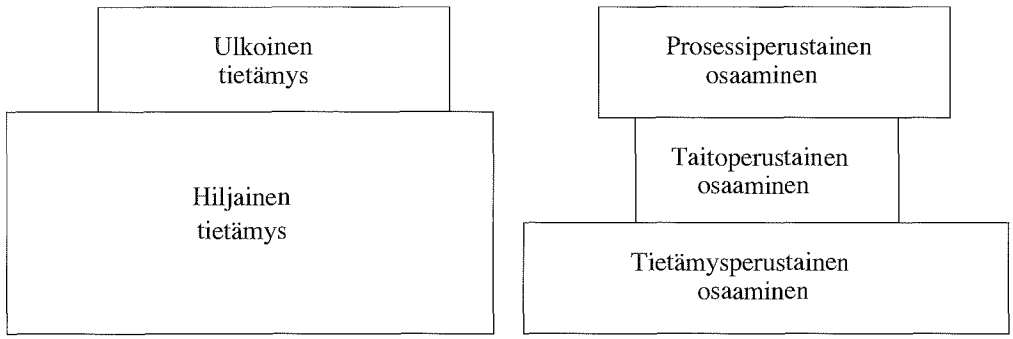
Tietoa voidaan jaotella paitsi hierarkkisesti, myös laadullisesti. Polanyi (1966) on esittänyt tiedon kahdeksi laadulliseksi ulottuvuudeksi ulkoisen tietämyksen (explicit knowledge) ja hiljaisen tietämyksen (tacit knowledge). Ulkoinen tietämys on esitettävissä olevaa objektiivista, rationaalista ja teoreettista tietoa. Hiljainen tietämys on subjektiivista, kokemuksiin perustuvaa käytännöllistä tietoa, jota on vaikeampi esittää eksplisiittisessä muodossa (Nonaka & Takeuchi 1995). Tietoverkot sisältävät esitettävissä olevaa ulkoista tietämystä. Vuorovaikutuksessa ihmisen kanssa tietoverkoissa oleva ulkoinen tietämys saattaa aktivoida ja jopa luoda myös hiljaista tietämystä.

Tiedon hierarkkisen luonteen mukaisesti tietoverkkojen sisältämä tieto on siis niihin tallennettua ja niissä liikkuvaa dataa ja sen pohjalta syntyvää informaatiota. Käsitteiden määrittely ei silti ole kovin yksiselitteistä: tieto -sanaa käytetään suomen kielessä monesti informaation synonyymina – puhutaanhan nykypäivän yhteiskunnastakin sekä tietoyhteiskuntana että informaatioyhteiskuntana. Tässä artikkelissa käytämme datasta, informaatiosta ja tietämyksestä sanaa tieto.

3.2.2 Osaaminen

Osaaminen tarkoittaa yksilön kykyä hyödyntää tietoa tehtävän suorittamiseksi. Yksilön osaaminen muodostuu Rasmussenin (1986) mukaan taito-, prosessi- ja tietämyspohjaisesta osaamisesta. Taito on kyky toimia ennalta määriteltyjen teknisten tai praktisten sääntöjen mukaisesti kuten kirjoitus- tai soittotaito. Prosessiperustainen osaaminen perustuu siihen, että yksilö tuntee päämäärän saavuttamiseksi tarvittavat vaiheet ja niiden järjestyksen kuten tuotteen valmistuksessa tarvittavan prosessin vaiheet ja niiden järjestyksen. Tietämysperustainen osaaminen tarkoittaa sitä, että yksilö itse tunnistaa toimintansa päämäärät ja muotoilee niiden perusteella toimintatavat. Tarvittava tietämys on esimerkiksi hyvin kehittyneitä malleja ongelma-alueesta ja toimintaympäristöstä sekä kyky arvioida erilaisten toimenpiteiden seurauksia. Osaamisen eri lajien sekä hiljaisen ja ulkoisen tietämyksen suhdetta toisiinsa on hahmotettu kuvassa 4.

Tietämysperustainen osaaminen ei ole vain tietämyksen omistamista vaan aktiivista ja dynaamista tietämistä. Esimerkiksi menestyksekäs tietoturvallisuusjohtaja tarvitsee kaikkia kolmea osaamisen lajia kyetäkseen suoriutumaan tehtävästään. Hänen on luonnollisesti oltava luku- ja kirjoitustaitoinen. Sen lisäksi hänen on kyettävä hyödyntämään organisaatiossa määriteltyä tietoturvallisuuspolitiikkaa. Muuttuva ympäristö kuitenkin tuo hänen eteensä päivittäin ongelmia, joiden ratkaisemisessa hän tarvitsee ennen kaikkea tietoturvallisuuden kysymyksiin liittyvää kokemusperäistä tietämystä.

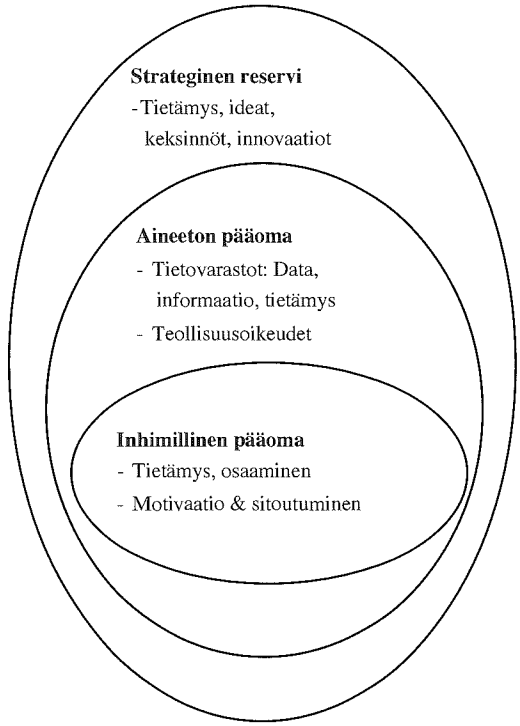


Kuva 4 Tietämyksen eri lajien sekä osaamisen eri lajien välinen suhde.

3.2.3 Tietopääoma

Tiedon johtaminen tarkoittaa organisaation tietovirtojen ja tietopääoman hallintaa. Organisaation tietovirtoja hallitaan tiedon tarpeet määrittelemällä, tietoja hankkimalla, organisoimalla, tallentamalla, jalostamalla, jakelemalla ja käyttämällä (Choo 1998). Ståhlen ja Grönroosin (1999) mukaan yrityksen tietopääoma muodostuu strategisesta reservistä, aineettomasta pääomasta ja inhimillisestä pääomasta (Kuva 5). Strateginen reservi on nimensä mukaisesti tarkoitettu käytettäväksi, mutta ei loppuun saakka kulutettavaksi ideoiden, keksintöjen ja innovaatioiden kasvuympäristöksi. Aineeton pääoma sisältää yrityksen teollisuusoikeudet sekä tietovarantoihin tallennetut datan, informaation ja tietämyksen. Inhimillinen pääoma sisältää henkilöstön tietämyksen ja osaamisen sekä

motivaation ja sitoutumisen. Tietoteknisten menetelmien avulla tapahtuvilta informaatiouhkilta suojautumissa keskeisintä on inhimillisen pääoman eli henkilöstön johtaminen. Strategista reserviä tarvitaan varsinkin uhkilta suojauduttaessa kun ideoidaan ja kehitetään uusia suojautumisen mahdollistavia lähestymistapoja.



Kuva 5 Organisaation tietopääoma (osit. Ståhle & Grönroos 1999).

3.2.4 Tiedon ominaisuudet tietoturvan kannalta

Tietoa kohtaan hyökättäessä pyritään vaikuttamaan sen ominaisuuksiin. Tietoturvan kannalta tiedon tärkeimmät ominaisuudet ovat tiedon luottamuksellisuus (confidentiality), eheys (integrity) ja saatavuus (availability). Tiedon luottamuksellisuudella tarkoitetaan sitä, että tiedot ovat vain niihin oikeutettujen henkilöiden saatavilla. Tiedon eheydellä tarkoitetaan sitä, että tiedot ovat totuuden mukaisia eivätkä muutu tai tuhoudu esimerkiksi inhimillisen toiminnan, laitteisto- tai järjestelmävian tai vihamielisen hyökkäyksen vuoksi. Tiedon saatavuudella tarkoitetaan sitä, että tiedot ja niiden muodostamat palvelut ovat niihin oikeutettujen henkilöiden käytettävissä ja saatavilla oikea-aikaisesti. (Waltz 1998)

Waltz (1998) viittaa lähteeseen (NSI 1995) ja kuvaa, että tiedon eheyteen läheisesti liittyviä käsitteitä ovat alkuperäisyys, koskemattomuus ja kiistämättömyys. Tiedon alkuperäisyydellä tarkoitetaan varmistumista siitä, että tieto on esimerkiksi tullut sieltä, mistä se näyttäisi tulleen. Tiedon koskemattomuus taas merkitsee, ettei tietoa ole missään vaiheessa muutettu laittomasti ja kiistämättömyyden avulla voidaan varmistua, että tieto on juuri sitä, mitä luulemme sen olevan.

Euroopan komissio (2001) määrittelee edellä mainitut tiedon ominaisuudet tietoturvallisuuteen liittyvien toimenpiteiden kautta. Luottamuksellisuudella tarkoitetaan tietojen suojelua luvattomalta sieppaukselta ja lukemiselta. Eheydellä tarkoitetaan lähetettyjen, vastaanotettujen ja tallennettujen tietojen täydellisyyttä ja muuttumattomuutta. Saatavuudella tarkoitetaan sitä, että tiedot ovat saatavissa ja palvelut toimivat häiriöistä, kuten virtakatkoksista, luonnonmullistuksista, onnettomuuksista tai hyökkäyksistä huolimatta.

3.2.5 Tietoturvallisuuden hallintajärjestelmä

Tietoturva-alan standardissa (BS7799-2:2002) määritellään miten tietoturvallisuuden hallintajärjestelmä rakennetaan, operoidaan, ylläpidetään ja parannetaan. Hallintajärjestelmän rakentaminen koostuu kuudesta vaiheesta, jotka ovat:

5 Tietoturvapolitiikan määrittely
6 Tietoturvallisuuden hallintajärjestelmän kattaman alueen määrittely
7 Riskien arviointi
8 Riskien hallinta
9 Valvonnan tavoitteiden ja keinojen valinta
10 Soveltuvuuslausunnon valmistelu

Näistä kohdista erityisesti jatkuva riskien arviointi ja riskien hallinta korostuvat kun suunnitellaan ja toteutetaan suojautumista tietoteknisten menetelmien avulla tapahtuvilta informaatiouhkilta.

3.3 Kriittinen infrastruktuuri ja tietoverkko

3.3.1 Tietoverkko

Euroopan komissio (2001) määrittelee tietoverkot järjestelmiksi, joissa tietoja tallennetaan ja käsitellään ja joiden kautta tiedot kulkevat. Tietoverkon osia ovat tiedonsiirtokomponentit kuten esimerkiksi kaapelit ja reitittimet, tukipalvelut kuten verkkotunnusjärjestelmät sekä verkkoon liitetyt päätelaitteet sovelluksineen. Valtiovarainministeriön (2002) mukaan tietoverkolla tarkoitetaan tiedonsiirtoverkon ja siihen kytkettyjen atk-laitteiden sekä ohjelmien muodostamaa kokonaisuutta, jolla välitetään tietoa muuten kuin tavanomaisena puhelinliikenteenä. Lisäksi tietoverkon avulla tarjotaan tiedonsiirtoon liittyviä palveluja kuten esimerkiksi osoite- muunnos- ja tietopalveluja sekä mahdollisesti myös asiakaspalveluja.

Vaikka esitetyissä määritelmissä ei suoraan korosteta ihmisten merkitystä tietoverkon osana, muodostuu tietoverkko vuorovaikutteiseksi systeemiksi vasta käyttäjiensä kautta. Ihmisten rooli on siis erittäin merkittävä, sillä tietoverkko itsessään on vain väline tiedon siirrolle ja tallennukselle. Tietoverkosta on nykyaikaisessa yhteiskunnassa muodostunut "informaatiosilta", jonka solmukohtia ovat muun muassa reitittimet, teleliikenteen solmukohdat, merkittävät tietovarastot ja keskeisimpinä ihmiset itse.

Tietoverkkoon on sitoutunut yhteiskunnan toimivuuden kannalta merkityksellistä tietoa sekä ihmisten että tietoverkon solmukohtien kautta. Päätehtävänsä mukaisesti tietoverkko välittää tietoa paikasta toiseen, mutta lisäksi se sisältää tallennettua tietoa esimerkiksi palvelimilla ja päätelaitteissa. Tiedot voivat olla yhteiskunnan kannalta kriittisiä

oman toiminnan ylläpitämisessä tai luonteeltaan sellaisia, että ne eivät saa päätyä väärien tahojen haltuun.

3.3.2 Yhteiskunnan infrastruktuuri ja kriittiset kohteet

Yhteiskunnan toiminnan kannalta keskeiseen infrastruktuuriin katsotaan kuuluvaksi (osit. Heiskanen 2001):

11 vesi- ja ruokahuolto
12 energian tuotanto ja siirto
13 liikenne- ja kuljetusjärjestelmät
14 rahaliikenne
15 teollisuuden tuotantolaitokset
16 tietoverkot

TIHA1 - työryhmän raportissa (2000) yhteiskunnan kannalta kriittisiksi kohteiksi määritellään turvallisuusviranomaiset, julkishallinnon organisaatiot, korkean teknologian yritykset, tieto- ja viestintäyritykset, pankit ja rahoitusyhtiöt sekä korkeakoulut ja oppilaitokset. Turvallisuusviranomaisiin kuuluvat valtion yleisestä turvallisuudesta ja järjestyksestä huolehtivat organisaatiot kuten poliisi, palo- ja pelastuslaitos sekä puolustusvoimat.

Infrastruktuuri/ välittömästi kriittinen kohde	Turval-lisuusvi-ranomaiset	Julkis-hallin-to	Korkea tekno-logia	Tieto- ja viestintä-yritykset	Pan-kit	Korkea-koulut
Vesi- ja ruoka	x	x	x	x	x	x
Energia	x	x	x	x	x	x
Liikennejär.	x					
Rahaliikenne					x	
Tuotanto-laitokset			x	x		
Tietoverkot	x	x	x	x	x	x

Kuva 6 Uhkakenttäanalyysi.

Infrastruktuurin ja kriittisten kohteiden välisiä suhteita on analysoitu oheisessa uhkakenttäanalyysissä. Vesi- ja ruokahuolto sekä energian tuotanto ja siirto on merkittävää kaikkien kriittisten kohteiden kannalta. Kriittiset kohteet ovat useimmiten kuitenkin varautuneet sekä vesi- ja ruokahuollon että ennen kaikkea energian tuotannon ja siirron häiriöihin. Käytössä on varajärjestelmiä, jotka toimivat yleisesti useita tunteja tai jopa päiviä. Liikenne- ja kuljetusjärjestelmien toimivuus on olennaisinta turvallisuusviranomaisille. Rahaliikenne on keskeistä ennen kaikkea pankeille ja rahoitusyhtiöille vaikkakin rahaliikenteen toimimattomuus haittaa suuresti kaikkien kriittisten kohteiden toimintaa. Tuotantolaitosten toimivuus on olennaista lähinnä korkean teknologian sekä tieto- ja viestintäalan yrityksille. Tietoverkkojen toimivuus on keskeistä kaikille kriittisille kohteille. Toimimattomille tietoverkon palveluille ei useinkaan ole helposti löydettävissä korvaavia palveluita. Esimerkiksi ylikuormitetun tai toimimattoman matkapuhelinverkon tu-

kiaseman alueella ei matkapuhelimen käyttäjälle ole tarjolla korvaavaa palvelua kiinteän puhelinverkon yleisöpalvelupisteiden poistamisen johdosta.

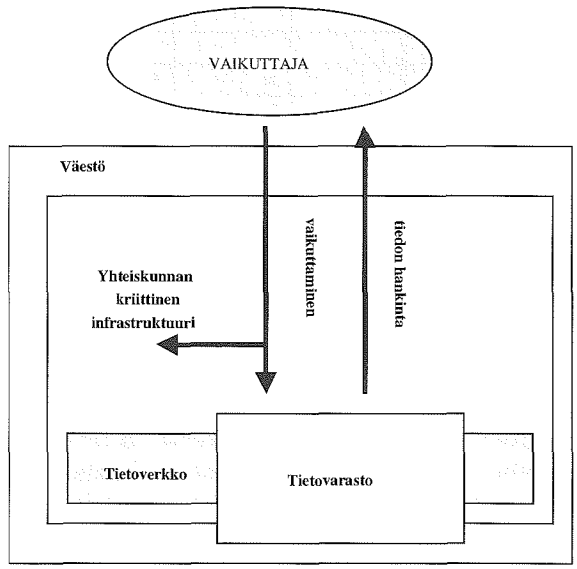
Petersen (1999) määrittelee teoksessaan Out of the Blue. How to Anticipate Big Future Surprices? niin sanottuja villejä kortteja (wild card), jotka tulevaisuudessa saattavat aiheuttaa haittaa yhteiskunnan toiminnalle. Petersenin esittämistä wild card –tekijöistä merkittävimmät ovat laaja sähköjärjestelmän rikkoontuminen, ongelmat tietoverkon toiminnassa, keskeisen informaatiojärjestelmän lamaantuminen sekä sähköisen rahajärjestelmän toimimattomuus.

Ristiintaulukoitaessa wild card –tekijöitä ja yhteiskunnan kannalta kriittisen infrastruktuurin osa-alueita, korostuu tietoverkon keskeinen merkitys mahdollisten informaatiouhkien kohteena sekä kanavana. Koska tietoverkko edellyttää toimiakseen sähköä, voi hyökkääjä myös laajalla sähköjärjestelmän lamauttamisella pysäyttää lähes kaikki yhteiskunnan keskeiset toiminnot.

3.4 Tietoon vaikuttaminen tietoverkon kautta

3.4.1 Tavoitteet tietoon vaikutettaessa

Koska tietoverkot ovat osa yhteiskunnan kriittistä infrastruktuuria, ne tarjoavat hyökkäävälle taholle sekä käyttökelpoista tietoa että välineen yhteiskunnan toimintaan vaikuttamiseksi. Yhä useammin itse tieto on myös hyökkäyksen kohde. Tietoon kohdistuvien hyökkäyksien avulla pyritään aina pohjimmiltaan vaikuttamaan tiedon luottamuksellisuuteen, eheyteen tai saatavuuteen ja niiden kautta ihmisten mielikuvanmuodostukseen. Keinoina hyökkäyksissä ovat tiedon salaus, harhautus ja tuhoaminen. Hyökkäyksen taustalla olevat motiivit vaikuttavat hyökkäyksen kohteen valintaan sekä hyökkäyksessä käytettävään menetelmään. Verkon kautta tapahtuvissa hyökkäyksissä on tiedonhallinnan kannalta tavoitteena joko kohdistaa haluttu vaikutus tietoon tai hankkia tietoa itselle.



Kuva 7. Hyökkääjän vaikuttaminen kriittiseen tietoon (Kuusisto 2002).

Hyökkääjä hankkii tietoverkon avulla käyttöönsä tietoa tietovarastoista. Hyökkääjä vaikuttaa joko välillisesti tietovarastoissa olevaa tietoa muuttamalla tai suoraan yhteiskunnan kriittisen infrastruktuurin toimintaan. Tiedon ominaisuuksiin vaikuttamisen tavoitteena voi olla joko kriittisen infrastruktuurin toiminnan lamauttaminen tai häiritseminen tai epävarmuuden luominen ja ihmisiin vaikuttaminen. Jälkimmäisessä tilanteessa hyökkääjä rikkoo tiedon saatavuuden sijaan tiedon eheyden. Tieto ei olekaan enää alkuperäistä, eli peräisin siitä lähteestä, josta se näyttäisi olevan. Lisäksi tiedon eheyteen kuuluva koskemattomuus on rikottu tietosisältöä muuttamalla. Samalla on rikottu myös kiistämättömyys, eli tieto ei ole sitä, mitä sen luullaan olevan. Hyökkääjän kannalta on edullista, jos kohde ei huomaa tiedon oikeellisuudessa mitään epäilyttävää. Psykologisessa vaikuttamisessa puhutaan refleksiivisestä kontrollista (Saarelainen 1999), joka tarkoittaa sitä, että vastustaja saadaan tekemään haluttu päätös tietämättään vaikutettavan saamaan tietoa kontrolloimalla.

3.4.2 Tietoverkko ja infrastruktuuri

Tietoverkon kautta tapahtuvissa hyökkäyksissä verkkoon vaikutetaan joko suoraan tai välillisesti. Suorassa hyökkäyksessä esimerkiksi tiedon kulkua voidaan haitata kuormittamalla reitittimiä turhalla liikenteellä. Välillisesti verkon toimintaan voidaan vaikuttaa kriittisen infrastruktuurin kuten esimerkiksi sähkönjakelun häirinnällä. Molemmissa on tavoitteena joko tietoverkon toiminnan vaikeuttaminen tai estäminen kokonaan.

Tietoverkon osista palvelimiin vaikutetaan verkon kautta esimerkiksi palvelunestohyökkäyksen avulla. Sen tavoitteena on palvelujen tai tiedon saatavuuden heikentäminen tai estäminen. Tällöin vaikutus kohdistuu tiedon saatavuuteen. Tiedon luottamuksellisuus taas voidaan rikkoa esimerkiksi tunkeutumalla autentikointipalvelimeen ja saamalla pääsy luottamukselliseksi tarkoitettuun tietoon. Laiton pääsy taas tarjoaa hyökkääjälle mahdollisuuden rikkoa tiedon eheys ja esimerkiksi vaikuttaa yhteiskunnan yksilöiden mieliin propagandan levittämisen tai dis-informaation jakamisen avulla.

Tietovarastot puolestaan sisältävät yhteiskunnan toimivuuden kannalta sekä julkishallinnon että yksityisen sektorin kriittisiä tietoja kuten esimerkiksi kansalaisten henkilötietoja, pankkitietoja, paikkatietoja ja yhteiskunnan toimivuutta koskevia suunnitelmia. Tällaisten tietojen joutuminen hyökkääjän haltuun aiheuttaisi suuren riskin yhteiskunnan turvallisuudelle.

Yhteiskunnan infrastruktuuriin liittyen valtion organisaatioiden rooli kansallisen toiminnan kontrolloijana on vähentynyt. Valtion kansallinen toimintakykyisyys riippuu siis yhä enemmän myös yritysmaailmasta. Esimerkiksi tiedon- ja sähkövoimansiirto-, kuljetus-, energia-, rahaliikenne- ja teollisuustuotanto -järjestelmistä sekä vesi- ja ruokahuollosta vastaavat etupäässä yksityiset yritykset. Suojautumisen informaatiouhkia vastaan tekee monimutkaiseksi myös se, että tietoliikenneverkot ovat useampien eri teleoperaattorien hallussa, eivätkä vain kansallisesti vaan myös kansainvälisesti.

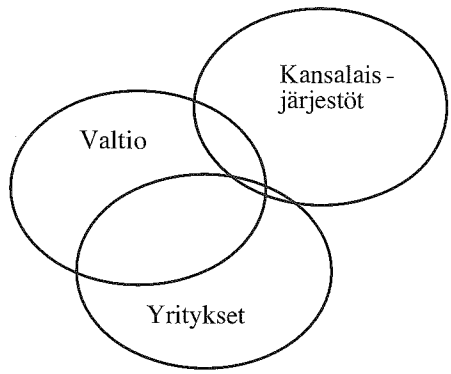
Tietoverkkojen yksityisessä omistuksessa ja hallinnassa oleminen sekä kansainvälistyminen ja muun infrastruktuurin riippuvuus tietoverkoista on huomioitu myös Euroopan komission tiedonannossa verkko- ja tietoturvasta (2001). Tiedonannossa todetaan, että edellä kuvatut asiat rajoittavat valtioiden kykyä vaikuttaa tietoverkkojen turvallisuuden

tasoon ja sitä kautta tiedon eheyden, luottamuksellisuuden ja saatavuuden säilyttämiseen. Globalisoituminen on siis nähtävissä myös tietoverkkoinfrastruktuurin osalta siirtymisenä suljetuista järjestelmistä kohti maailmanlaajuisia avoimia järjestelmiä. Tämän vuoksi yhteiskunnan toimivuuden kannalta kriittisen tiedon suojaaminen hyökkäyksiltä edellyttää valtionhallinnon ja yritysten tiivistä yhteistyötä sekä kansallisesti että kansainvälisestikin. Tietoverkkojen infrastruktuurin ulkomainen omistus saattaa tulevaisuudessa muodostua uhaksi, mutta toisaalta Suomessa fyysisesti sijaitseva verkko voidaan kriisitilanteessa ottaa hallintaan mikäli riittävä osaamistaso on kansallisesti olemassa. Siitäkin huolimatta tietoverkkojen kuuluminen yhteiskunnan kriittiseen infrastruktuuriin mahdollistaa hyökkääjälle teoriassa jopa valtion informaatiosaarron. Tämä on ollut informaatiosodankäyntiä toteuttavan hyökkääjän keskeinen tavoite lähes kaikissa vuoden 1990- jälkeisissä merkittävissä kansainvälisissä kriiseissä (Ahvenainen 2002b).

3.5 Tiedon merkitys tulevaisuudessa

Tulevaisuuden ennakointi yleensä ja erityisesti teknologian osalta on ongelmallista, koska muutosnopeus on suuri ja muutokseen vaikuttavia tekijöitä on useita. Voidaan kuitenkin ennustaa, että tietoverkkoinfrastruktuuri tulee olemaan entistä tärkeämpi perusta yhteiskunnan eri toiminnoille. Siten tietoverkko muodostaa myös yhä merkittävämmän sodankäynnin taistelukentän. Koska yhteiskunnan toiminnot ovat tiukasti sidoksissa tietoverkon toimintaan, voidaan verkkoon vaikuttamalla hyökätä koko yhteiskuntaa vastaan.

Edelliseen liittyen Alvin ja Heidi Toffler (1994) kuvaavat kirjassaan Sodan ja rauhan futurologia kolmannen aallon sodankäyntiä, jota ilmentävät tietoverkkoterrorismi, propaganda ja todellisuuden vääristyminen psykologisen sodankäynnin avulla. Kolmannen aallon tietämysorientoituneet yhteiskunnat eli tietoyhteiskunnat, joihin Suomikin lukeutuu, ovat haavoittuvampia ulkoisille uhkille kuin maatalous- tai teollisuusyhteiskunnat. Tietoyhteiskunnat tarvitsevat pääsyn kansainvälisiin tietoliikenneverkkoihin ja tietovarastoihin pysyäkseen toimintakykyisinä. Tofflerien näkemys tukee ajatusta, että tulevaisuudessa tietoyhteiskunta ei voi olla toimiva ilman tietoverkkoa.



Kuva 8 Tulevaisuuden toimijoita ovat valtion lisäksi yritykset ja kansainväliset organisaatiot sekä kansalaisjärjestöt (Kuusisto 2002).

Tiedon merkitys yhteiskunnan toiminnassa korostunee tulevaisuudessa vielä nykyistäkin enemmän. Tietoverkoilta vaadittanee yhä kehittyneempiä tapoja globaalisti tukea tietovirtoja ja niiden hallintaa. Tietovirrat liikkuvat sekä eri toimijoiden ja toimijaryhmien välillä että yhden toimijaryhmän sisällä (Kuva 8). Toimijaryhmät levittäytyvät eri paikkoihin riippumatta nykyisistä valtioiden välisistä rajoista. Tulevaisuudessa tietovirtojen liikkumisen ymmärtäminen on keskeistä informaatiouhkilta puolustauduttaessa. Ymmärtäminen edellyttää syvällistä tietämystä sekä ihmisen toiminnasta että tietoverkoista.

LÄHTEET

Ahvenainen, S. (2002a): Kirjeenvaihtoa artikkelin teemasta. Julkaisematon.

Ahvenainen, Sakari (2002b): Sähköisen joukkoviestinnän merkitys tietosodankäynnissä ja viimeaikaisten sotien opetukset oman toiminnan turvaamisesta poikkeusoloissa. Loppuraportti Puolustustaloudellisen Suunnittelukunnan joukkoviestintätoimikunnalle 5.9.2002.

British Standard BS7799-2:2002.
http://www.gammassl.co.uk/topics/hot1.html 14.11.2002

Choo, C. 1998: The knowing organization. How Organizations Use Information to Construct Meaning, Create Knowledge and Make Decisions. Oxford University Press. 298 s.

Davenport, T & Prusak, L. 1998: Working knowledge. How organizations manage what they know. Harvard Business School Press. USA. 199 s.

Euroopan komissio. 2001: Verkko- ja tietoturva: Ehdotus eurooppalaiseksi lähestymistavaksi. Euroopan komission tiedonanto neuvostolle, Euroopan parlamentille, Euroopan talous- ja sosiaalikomitealle sekä alueiden komitealle. KOM(2001)298 lopullinen. Bryssel 06.06.2001. 28 s. http://europa.eu.int/eur-lex/fi/com/cnc/2001/com2001_0298fi01.pdf 13.01.2002

Halonen, K. 2000: Operatiivinen turvallisuus teoksessa Johtamissodankäynti, seminaariaineisto. Maanpuolustuskorkeakoulun Taktiikan laitos julkaisusarja 2 n:o 2/2000. ISBN 951-25-1187-8.

Hammond, G.T. 2001:The Mind of War; John Boyd and American Security. Smitsonian Institution Press, Washington and London. 190 s.

Heiskanen, M. 2000. Informaatiosodankäynti johtamissodankäynnin yläkäsitteenä. Maanpuolustuskorkeakoulun taktiikan laitoksen johtamissodankäynnin seminaari 26. – 27.10.2000. 31 s. http://www.telecomlab.oulu.fi/home/coursematerial/Johtamissodank%E4ynti_IW.pdf 30.01.2002

Kuusisto, R. 2002: Haastattelumuistiinpanoja. Julkaisematon.

Niiniluoto, I. 1997: Informaatio, tieto ja yhteiskunta. Filosofinen käsiteanalyysi. Edita. Helsinki. 136 s.

Nonaka, I. & Takeuchi H. 1995: The knowledge creating company. Oxford University Press. USA. 284 s.

National Security Institute (NSI) 1995: http://nsi.org/Library/Compsec/nii.txt

Puolustustaloudellinen suunnittelukunta, Tietojärjestelmäjaosto, Tiedonsiirtotoimikunta. 2001: Tiedonsiirron ja –käsittelyn muutos- ja uhka-analyysi 1/2001. Seurantaraportti 26.09.2001. Helsinki. 8 s. www.nesa.fi 23.01.2002

Pöyhönen, T. 1998: Evl. S. Ahvenaisen muistiinpanot FT T. Pöyhösen luennoista 24.-26.4.1998 Vierumäellä. FT T. Pöyhönen esitti tekemisen edellytykset, jotka olivat: Osaaminen, jaksaminen, halu tehdä ja uskallus tehdä. Julkaisematon.

SITRA. 2001: Suomi 2015. Suomen tulevaisuuden menestystekijät ja haasteet. Suomi 2015 -ohjelman 3. kurssin loppuraportti. Sitra. Helsinki. 18 s. http://194.100.30.11/suomi2015/suomi2015_3/index.html 22.3.2002

Rasmussen, J. 1986: Information Processing and Human-Machine Interaction: An Approach to Cognitive Engineering, North Holland.

Ståhle, P. & Grönroos, M. 1999: Knowledge Management, Tietopääoma yrityksen kilpailutekijänä. Suomi.

Tietoturvallisuuden hallinnointi 1 – työryhmä (TIHA1). 2000: Tietojärjestelmien tietoturvallisuuden hallinnolliset järjestelyt. Puolustustaloudellisen suunnittelukunnan TIHA1-työryhmän raportti 15.05.2000. 44 s.

Thierauf, R. 2001: Effective Business Intelligence Systems. London. Quorum Books. 370 p

Toffler, A. & Toffler, H. 1994: Sodan ja rauhan futurologia. Suomentaneet Kerkkonen J. ja Sauri S. Kustannusosakeyhtiö Otava. Keuruu. 332 s.

Valtiovarainministeriö - Hallinnon kehittäminen – Tietohallinto.
Ei päiväystä. Tietoturvasanasto
http://www.vn.fi/vm/kehittaminen/tietoturvallisuus/vahti/sanasto/sisallys.htm 13.01.2002

Waltz, E. 1998: Information Warfare. Principles and operations. Artech House. Boston. London. 397 s.

4. MITEN TEKISIN VERKKOHYÖKKÄYKSEN ?

Mikko Hyppönen
Tutkimuspäällikkö,
F-Secure Oyj

Tämä artikkeli pyrkii vastamaan seuraaviin kysymyksiin;

- miten vihollisen kannattaisi tehdä verkkohyökkäys Suomi Oy:tä vastaan nyt ja tulevaisuudessa
- miten verkkohyökkäys kannattaisi organisoida ja toteuttaa
- mitkä olisivat verkkohyökkäyksen kohteita eri vaiheissa

Verkkotaistelussa hypoteesina on kolme erilaista skenaariota:

- täsmähyökkäys
- maan lamautus verkostollisella doktriinilla
- taloudellinen isku

4.1 Taustaa

Tätä kirjoitettaessa eletään vuotta 2003. Vuoteen 2020 on siis 17 vuotta aikaa. Jos joku yritti 17 vuotta sitten, eli vuonna 1986 hahmotella vuoden 2003 tietoverkkosodankäynnin mahdollisia tekniikoita, tehtävä olisi ollut hyvin vaikea - liki mahdoton. Toisaalta tietotekniikan perussuuntaukset kuten verkottumisen lisääntyminen ja tietojenkäsittelytehon lineaarinen kasvaminen olivat nähtävissä jo 1980-luvun puolivälissä. Internetkin oli jo olemassa.

Miltä tietojärjestelmät näyttävät vuonna 2020? Entä internet? Miten tyypillisen kodin tai toimiston tekniikka on muuttunut? Kuinka riippuvainen koko yhteiskunta on tietokoneista?

Tätä tutkimusta varten teemme muutamia perusolettamuksia:

- Tapahtuma-aika on vuoden 2020 kesä.
- Suomi on säilynyt poliittisesti ja puolustuksellisesti riippumattomana
- Venäjä on edelleen suomen suurin puolustuksellinen uhka

Sekä lisäksi useita teknologiaa koskevia olettamuksia:

- Neljännen sukupolven kolmiulotteiset muistisirut[1] ovat vapaasti saatavilla ja halpoja. Mustamäen torilta voi ostaa 500 Eurolla sokeripalan kokoisen muistipiirin joka sisältää DVDX-tasoiset piraattikopiot kaikista Hollywood-elokuvista vuosilta 1970-2020. Kaupan päälle saa toisen piirin jolta löytyy MP8-musiikkikopiot käytännössä kaikesta länsimaissa koskaan julkaistuista musiikkilevyistä

- Toimivia kvanttitietokoneita[2] on olemassa, mutta ne ovat ilmeisesti kaikki Yhdysvalloissa. Kvanttikoneiden takia esim. 2048 bitin RSA-salausta ei enää pidetä turvallisena
- Televisiokuvan luotettavuus on hävinnyt. Koneiden laskentateho riittää hyvin siihen, että elokuvien päähenkilöt voidaan vaihtaa lennossa, ts. katsoja voi valita elokuviin lempinäyttelijänsä (tai vaikkapa itsensä) jotka hänen kotisoittimensa renderoi reaaliajassa näytölle täysin luontevana
- Kaikki langaton puheluliikenne on kulkenut jo pitkään IP-verkkoliikenteenä. Langalliset puhelinliittymät ovat käytännössä hävinneet
- Suurin osa tyypillisen kodin kodinkoneista on kiinteässä yhteydessä internetiin ja sitä kautta hallittavissa kännyköiden ja verkkokonsolien kautta

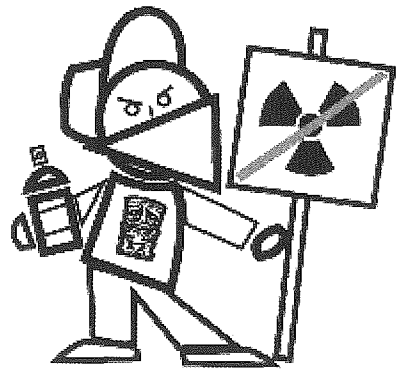
- Yli 95% suomalaisista kodeista on vähintään 10MB kiinteällä linjalla kiinni internetissä
- Yritysympäristöissä etätyöskentely on hyvin yleistä tehokkaiden verkkoliittymien ansiosta
- Microsoftin markkinaosuus työasemakäyttöjärjestelmissä on 90%, Linuxilla 10%
- Microsoftin markkinaosuus palvelinkäyttöjärjestelmissä on 75%
- Suurin osa televisio-ohjelmista jaellaan internetin kautta perinteisten jakelukanavien sijasta
- Lapset oppivat maailmankieli englannin tyypillisesti jo 4-5 vuotiaina ja seuraavat luontevasti kansainvälistä uutisvirtaa, lastenohjelmia ja nettiliikennettä. Paikallinen uutisointi kyseenalaistetaan helposti ja lisätietoja haetaan netitse ulkomailta
- Ostosten teko verkon kautta on arkipäiväistynyt. Noin 40% kaikesta kuluttajakaupasta käydään internetin kautta

- Suomalaispankkien kehittämä Nettilompsa(TM) -verkkoraha on yleistynyt, ja yli 90% verkkokaupoista maksetaan tällä virtuaalirahajärjestelmällä
- Suomen suurin yritys on Kapula Oyj, globaali matkapuhelin- ja tietoliikenneverkkoja ja niiden päätelaitteita valmistava jättiyritys. Kapula on myös merkittävä puolustusjärjestelmien valmistaja

4.2 Skenaario 1: täsmähyökkäys

Tässä skenaariossa tehokkaasti organisoitu aktivistijärjestö ACTNOW tekee täsmähyökkäyksen suomalaisia pankkijärjestelmiä vastaan. Hyökkäyksen motivaationa on protestoida kaupallista elämänmenoa vastaan, kritisoida globalisaatiota ja levittää epäluottamusta rahalaitoksia kohtaan. Hyökkäyksen tavoitteena on haitata pankkien toimintaa mahdollisimman monella eri tavalla ja täten kostaa koko yhteiskunnalle sen piittaamattomuus ACTNOW:n edustamaa asiaa kohtaan.

ACTNOW on suomen sisällä toimiva ei-sotilaallinen ryhmä, jolla on runsaasti yhteyksiä ulkomaille. Ryhmän rahoitus tulee ilmeisesti maan rajojen ulkopuolelta. Ryhmään kuuluu useita tuhansia aktiivisia jäseniä, joista useimmat elävät modernin yhteiskunnan ulkopuolella. Merkittävä osa ryhmän jäsenistä on kuitenkin taustaltaan korkeasti koulutettuja ja teknisesti taitavia. Ryhmää johtaa karismaattinen johtohahmo.



Hyökkäys alkaa Kansainvälisenä maan päivänä, 22.4.2020.

4.2.1 Hyökkäystekniikat

- Koordinoitu valmistelu - raju lyhytaikainen isku
- Nettilompsa(TM) -verkkorahan arvon romahduttaminen "painamalla" miljardeja vääriä rahaa
- Hajautetut palvelunestohyökkäykset eri puolilta maailmaa, kohteena suomalaisten pankkien verkkopalvelut
- Täsmävirukset pankkien tietojärjestelmiä vastaan
- kriittisten tietokantojen muokkaus tai tuhoaminen myös organisaation sisältä käsin
- Asiakastietokantojen varastaminen ja luottamuksellisten tietojen laittaminen julkiseen levitykseen

- ACTNOW-propagandan uittaminen internet-tv-kanaville tietomurtojen kautta, alkuperäisten ohjelmien keskelle
- Informaatioarvon hyväksikäyttö - ACTNOW tiedottaa jatkuvasti tapahtumista STT:lle, MTV3:lle, iCNN:lle, AP:lle ja Reutersille

Hyökkäys kestää tasan viikon. 29.4.2020 ACTNOW:n johtaja ilmoittaa että ryhmän tavoitteet on saavutettu ja uhoaa miten pankkien kaataminen oli vasta alkua - "samoin käy kaikille muillekin tahoille jotka jättävät mielipiteemme huomiotta".

4.2.2 Hyökkäyksen seuraukset

Hyökkäyksen loppumisesta huolimatta pankkijärjestelmät eivät palaa ennalleen. Yksityisten ja yritysten maksuliikenne takkuilee ja pankkitalletusten mystisistä arvomuutoksista kinastellaan. Luottamus Nettilompsaa kohtaan katoaa ja järjestelmä ei koskaan enää yleisty uudelleen. Valtaosa palkansaajista ilmoittaa haluavansa palkkansa käteisenä rahana koska pankkeihin ei enää luoteta. Myös jalometallien hamstrausta tavataan. Inflaatio uhkaa karata käsistä. Osa kansainvälisistä yrityksistä ilmoittaa vetävänsä toimintonsa pois suomesta. HEX-indeksi laskee hyökkäysviikon aikana 22%, HEX-TECH yli 30% ja pankki- ja rahoitussektorin indeksi yli 50%.

4.3 Skenaario 2: maan lamautus verkostollisella doktriinilla

Tässä skenaariossa eräs iso valtio (tästä eteenpäin valtiosta käytetään nimiytstä Keltainen) pyrkii lamauttamaan Suomen valtion käyttäen sekä verkkohyökkäyksiä että perinteisiä hyökkäyksiä. Hyökkäyksen motiivina on maiden väliset tulehtuneet suhteet ja Keltaisen halu miehittää merkittäviä osia Suomesta.

4.3.1 Hyökkäystekniikat

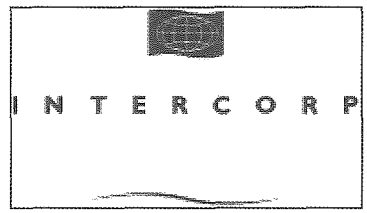
- Keltainen on soluttanut vakoojakoulutuksen saaneita ohjelmoijiaan Microsoftille töihin jo vuosikymmenten ajan. Kyseiset henkilöt ovat piilottaneet yleisimpien käyttöjärjestelmien sisään loogisia pommeja joiden etäaktivointi on helppoa ja joiden kautta näennäisen suljettuihin järjestelmiin on helppo tunkeutua ulkopuolelta
- Merkittävien tietovarastojen (suuret it-palvelutalot, integraattorit, suuryritykset, väestörekisteri, verottaja, pankit) tuhoaminen loogisilla pommeilla
- Tärkeimpien tietovarastojen (kuten sähkö- ja vesihuolto) tuhoaminen fyysisillä pommeilla. Sisältää tiedustelulla selvitettyjen varmuuskopiosijoituspaikkojen tuhoamisen.
- Lukuisten tietohallintopäälliköiden, asiantuntijoiden ja kriittisiin tehtäviin kriisin aikana sijoitettujen ihmisten eliminointi
- Dis-informaatiosodankäynti
- Nopea taistelutempo
- Vaikutuksen synkronointi
- HPM-aseiden käyttö järjestelmien tuhoamisessa
- DDoS hyökkäysten laukaiseminen muuta maailmaa vastaan suomalaista koneilta, pakottaen muun maailman eristämään suomen verkkoliikenteen

4.3.2 Hyökkäyksen seuraukset

Taistelu kestää viikkojen ajan. Suomen joukkojen toimintaa vaikeuttaa siviilipuolen sekasorto telekommunikaation hävittyä koko maasta. Siviilipuolen moraali on alhaalla kun perusinfrastruktuuri häviää heti kättelyssä. Uhkana sodan häviäminen.

4.4 Skenaario 3: taloudellinen isku

Tässä skenaariossa kansainvälinen INTERCORP GROUP -yritys käyttää verkkosodankäynnin menetelmiä suomen teollisuuden johtotähteä, Kapula Oyj:tä vastaan. Kyseessä on ennen kaikkea taloudellinen isku, jonka tarkoituksena on haitata Kapulan toimintaa ja karkottaa sen asiakkaita.



4.4.1 Hyökkäystekniikat

- Kansainvälisen tietoliikenteen haittaaminen
- Yrityksen verkkopalveluiden kaappaaminen ja yrityksen maineen mustamaalaaminen
- Verkkoruuhkat
- Telekommunikaatiokatkokset
- Yrityksen vastainen propaganda ja psykologiset operaatiot
- Hyökkäykset kestävät kuukausia, jopa vuosi
- Huolella organisoitu ja salattu toiminta
- Tietomurrot
- Teollisuusvakoilu
- Avainhenkilöiden pelottelu, murhaaminen

4.4.2 Hyökkäyksen seuraukset

Kapula Oyj toiminnan vaikeutuminen vaikuttaa koko maan talouteen - lama. Muiden yritysten pako Suomesta kiihtyy. Uusi uhkakuva aiheuttaa ongelmia puolustukselle

4.5 Yhteenveto

Tietoverkkojen tehtävien hyökkäysten uhkakuvat näyttävät muuttuvan vuosi vuodelta pahemmiksi. Edelleen pitäisi muistaa että jos kaivataan todellista, korkean tason tietoturvaa, käytettävät tietokoneet pitäisi kokonaan eristää julkisista verkoista.

5. MITEN VERKKOTAISTELUSSA PUOLUSTAUDUTAAN ?

Professori Jorma Jormakka
Tekniikan laitos
Maanpuolustuskorkeakoulu

5.1 Johdanto

Tämä luku pyrkii vastaamaan kysymykseen, kuinka voidaan puolustautua edellisessä luvussa esitettyihin hyökkäyksiin. Nämä hyökkäykset eivät ole olleet käytettävissä tätä kirjoitettaessa, joten puolustusmenetelmissä on tukeuduttu valittuihin uhkaskeraarioihin, jotka tässä lyhyesti kuvaillaan.

Skenaario 1.
Asevoimiltaan teknisesti heikompi maa, terroristiorganisaatio tai muu ryhmittymä tekee EU:n alueen maissa yhteiskuntaan kohdistuvan hyvin suunnitellun ja valmistellun tietoverkkohyökkäyksen. Tällainen hyökkäys tehdään tarkkaan valittuna aikana koska hyökkäyskeinot toimivat vain jos sopivia aukkoja on. Hyökkäys on todennäköisesti ensi-isku.

Skenaario 2.
Asevoimiltaan teknisesti kehittynyt maa tekee asevoimin hyökkäyksen Suomeen. Hyökkäys alkaa vaiheella, jonka tarkoitus on lamaannuttaa vastustajan yhteiskunnan elintärkeät osat ja puolustusvoimien johtamisjärjestelmä. Tähän käytetään pääosin ilmaiskua. Verkkosodankäynti tukee hyökkäystä.

Skenaario 3.
Toinen maa ja suuri yritys pyrkii aikaansaamaan taloudellisia menetyksiä suomalaisissa yrityksissä vetkkosodankäynnin menetelmin. Päämääränä voi olla maan heikentäminen strategisista syistä.

Näistä skenaarioista puuttuu verkkosodankäynnin kannalta luonnollinen skenaario, jossa Suomi vastaa Skenaarioon 2 verkkosodankäynnin menetelmin. Tämä, luonteeltaan vastahyökkäyksen kaltainen puolustusskenaario on kuvattu seuraavassa:

Skenaario 4.
Suomi joutuu Skenaarion 2 hyökkäyksen kohteeksi. Koska hyökkääjä on tässä skenaariossa tunnistettavissa, Suomi käynnistää, muiden vastatoimien rinnalla, vastahyökkäyksen verkkotaistelun avulla. Verkkotaisteluskenaario on luonteeltaan Skenaarion 1 mukainen, mutta eroaa siinä, että se kohdistuu myös vastustajan puolustusvoimiin,

psykologisilla operaatioilla mielipiteen vaikuttamiseen on olennaisempi osa sekä siinä suhteessa, ettei hyökkäysaikaa voi yhtä vapasti valita. Vastahyökkäys ei siis ole samassa mielessä valmisteltu kuin Skenaario 1 joten se on teholtaan pienempi. Tämä suuntaa vastahyökkäystä enemmän yhteiskunnassa oleviin heikosti suojattuihin maaleihin ja toiminnan päämääränä on selvemmin kaaoksen aiheuttaminen ja sitä kautta mielipiteeseen vaikuttaminen.

Puolustusmenetelmissä 2020 on otettava huomioon tietoverkon kehitys vuoteen 2020 mennessä, nykyisin tunnetut tietoturvamekanismit ja niiden puuttteet, mahdolliset uudet tietoturvamekanismit vuonna 2002, joista tässä esitetään ns. palveluverkko-konsepti. Näiden pohjalta esitetään lopuksi puolustusmenetelmät eri uhkaskenaa-rioille.

5.2 Tulevaisuuden tietoverkko

Kappale kuvailee tulevaisuuden tietoverkon rakenteen nykyisten käsitysten valossa. Tieto- ja tietoliikennetekniikan ennustaminen 20 vuoden aikajänteellä on erittäin vaikeaa. On selvää, että uusia teknologioita kehitetään tällä aikataululla. Tietyttyjä trendejä voidaan pitää luultavina.

5.2.1 Trendit

1. Mobiilin pääsyn lisääntyminen. NMT:n (Nordic Mobile Telephone) ja GSM:n (Global Service for Mobile networks) aloittama langattoman puhelimen yleistyminen jatkuu näiltä näkymiltä. 4G verkkotekniikoissa langaton rajapinta usein nähdään WLAN (Wireless Local Area Network)-tekniikalla toteutettavaksi, mutta muitakin tekniikoita tarvitaan. Puhelin saa täydet tietokoneen ominaisuudet. Näyttöpääte ja näppäimisto ovat suurin ongelma, mutta näytöt ovat jo nyt sangen riitäviä ja näppäimistön osalta puheohjattu datan syöttö on eräs vakavasti otettava mahdollisuus.

2. Palveluiden merkitys kasvaa johtuen tietoverkon yli käytetyttyjen tietoteknisisten sovellusten kehittymisestä. Palvelut nähdään liiketoiminta-alueena joiden merkitystä kasvattaa se, että kilpailun lisääntyminen, teletoiminnan vapauttaminen ja uusi tekniikka johtaa tiedon siirron hintojen laskuun. Tekniikan laskeva vaikutus hintoihin perustuu osin myös siihen, että IP (Internet Protocol) liikenteen laskuttaminen on huomattavasti vaikeampaa ja työläämpää kuin PSTN (Public Switched Telephony Network) liikenteen, joten laskutuksessa suositaan kiinteää hintaa tai muita helposti toteutettavia ratkaisuja. Operattoreiden on toimintansa ylläpitämiseksi kehitettävä uusia tulolähteitä. Mikäli niitä ei löydy, operaatorit eivät voi alhaisilla hinnoilla pitää yllä verkkoja ja niiden kehitystä, mikä johtaa hintojen kasvuun. Luultavimpana ratkaisuna nähdään palvelut ja niistä laskuttaminen. Kaikkien yhteiskunnan toimintojen siirtyminen tietoverkkoon on jo alkanut ja kehitys jatkunee.

3. Laajakaistaiset palvelut yleistyvät. Vaikka kuvapuhelinta on yritetty jo 20 vuotta, niin se ei ole yleistynyt. Ongelma palautuu kuitenkin pääosin hintaan, joka edelleen on korkea, tai laatu huono mikäli hinta on alhainen. Trendi seuraa siirtonopeuksien kasvusta. On todennäköistä että tulevaisuuden sovellutukset löytyvät kyllä

joukosta: (kiinteä tai mobiili) videopuhelin, videokonferenssi, etätyö, etäkoulutus, etäsairaanhoito, vanhusten- lasten ja vammaisten etähoito, videokuvan tai stillkuvan lähetys mobiilista esimerkiksi matkalla, sähköinen kaupankäynti mobiilista tai kiinteällä yhteydellä, television- ja radiolähetykset verkossa. Näitä sovelluksia joudutaan parantelemaan joillakin uusilla ajatuksilla, koska kaikkia on jo kehitetty 10-5 vuotta, mutteivät ne ole lähteneet vielä nousuun. Reaaaliaikavideokuvan siirto ei yleisty aivan lähiaikoina koska IP-verkko, jota nyt rakennetaan runkoverkoksi ei pysty välittämään suurta määrää reaaliaikaista videokuvaa kehitetyilla palvelunlaadun tekniikoilla ja samalla saavuttaa korkeaa verkon käyttöastetta. IP-runkoverkossa on otaksuttu, että pääosa liikentestä on jatkossakin interaktiivista dataliikennettä (mukaanlukien varastoitu video-kuva), ja reaaliaikaliikenne on lähinnä IP-puhetta, joka tarvitsee vain pienen kaistan. Luultavasti runkoverkko joudutaan suunnittelemaan uudestaan ennen 2020 aikarajaa.

5.2.2 Siirtoverkko

Kiinteä siirtoverkko kehittyy kohti täysin optisia verkkoja. Nykyiset verkot käyttävät SDH (Synchronous Digital Hierarchy)-siirtojärjestelmää, mutta optisen siirtoverkon (OTN) tekniikat WDM (Wavelength Division Multiplexing) ja DWDM (Dense-WDM) ovat jo laajalti toiminnassa suuremmilla siirtonopeuksilla. GFP (Generic Framing Procedure) on kehitetty sovittaman IP data SDH-kehyksiin, mutta GFP toimii myös suoraan OTN:n (Optical Transfer Network) päällä ja jatkossa SDH todennäköisesti väistyy ja korvautuu GFP:llä. ATM (Asynchronous Transfer Mode) on toistaiseksi laajalti käytössä runkoyhteyksillä SDH:n päällä, mutta se myös korvautuu GFP:llä, jonka päällä on MPLS (Multi-Protocol Label Switching) tai GMPLS (Generic MPLS). GMPLS on MPLS:n laajennus, jolla voidaan erottaa leimapolkuja OTN:stä ja kytkeä esimerkiksi aallonpituuksia tai kuituja. GMPLS on hyvin todennäköinen tekniikka OTN:n päällä. Täysin optiset siirtoverkot, joissa myös kytkimet ovat optisia on todennäköisesti käytössä jo 2020.

5.2.3 Verkkokerros

Verkkokerros on muutaman vuoden päästä IP-pohjainen, mutta nykyiset verkkotekniikat säilyvät vielä pitkään käytössä: tulevaisuuden verkko on siis erilaisten yhteentoimivien verkkojen yhdistelmä. IP-tekniikan ongelmat: palvelunlaatu, turvallisuus ja laskutus voidaan ratkaista riittävässä määrin, vaikka toistaiseksi esitetyt ratkaisut eivät olekaan täydellisiä. Reititin kehittynee enemmän ohjelmoitavaksi kytkimeksi (Softswitch) NGN arkkitehtuurin mukaisesti. Softswitch usein ymmäretään synonyymiksi MGC (Media Gateway Controller) verkkosolmulle, joka yhdistää IP-verkon ja jonkin muun verkon merkinannon, mutta tässä termi tarkoittaa ohjelmoitavan rajapinnan tarjoavaa verkkosolmua, jonka päälle voi rakentaa puheluiden lisäarvon palveluita joustavasti, siis Softswitch voi tarkoittaa myös esimerkiksi JTAPI (Java Telephony Application Programming Interface) -rajapinnan tarjoavaa SIP (Signalling IP)-palvelinta. Palvelun laatu IP verkossa on tarpeen VoIP:n (Voice over IP) toteuttamiseksi. Palvelun laadun mahdollistavista tekniikoista DiffServ (Differentiated Services) on luultavin, joskin on mahdollista, että MPLS ja riittävän löysä mitoitus antavat riittävän laadun ilman varsinaisia QoS (Quality of Service) IP protokollia. Sangen yleinen on myös käänteinen ennuste: MPLS ja mitoitus on QoS:n päätekniikka, joskin DiffServ voi myöskin olla joissain verkoissa mukana. IP-runkoverkossa tarvitaan lisäksi joukko palvelimia, esimerkiksi DNS (Domain Name Server), AAA (Aut-

hentication, Authorization, Accounting), LDAP (Lightweight Directory Access Protocol) ja PBN (Policy Based Networking) palvelimia.

5.2.4 Palveluteknologiat

Lisäarvon palveluiden luonti tulevaisuuden VoIP/SIP verkossa perustunee seuraaviin tekniikoihin: Java servlets ja JavaBeans komponentit, CPL (Call Processing Language) ja muut XML (Extensible Markup Language)-pohjaiset skriptikielet, Parlay/OSA (Open Service Architecture) API sekä MExE/SAT (Mobile Execution Environment ja SIM Card Application Toolkit) palvelimet ja mobiilissa sijaitsevat sovellukset. Nämä tekniikat mahdollistavat nopean palvelunluonnin, joka on olennaista taloudellisesti kannattavien palvelujen kehittämiseksi. Palvelutekniikoiden tietoturvauhkia vähentää se, että niissä on mukana sangen hyvät tietoturvamallit. Toisaalta mikäli tietoturvamalli murretaan, nämä tekniikat mahdollistavat esimerkiksi henkilön paikallistamisen, hätäpuheluiden ruuhkaannuttamisen, erilaisten käyttäjistä kerättyjen tietojen ja tunnisteiden paljastumisen ja ehkä jopa päätelaitteiden käytön vakoiluun.

5.2.5 Verkonhallinta

Verkonhallinnan osalta TMN (Telecommunication Management Network) on edelleen käytössä PSTN:ssä ja GSMssä, mutta se muuttunee middleware-pohjaisiin ratkaisuihin. Näitä on valmistajakohtaisia, kuten IBM:n Tivoli, mutta standardin mukainen ratkaisu CORBA TMN (Common Object Request Broker Architecture based TMN, CMISE on CORBA) lienee kuitenkin varteenotettava vaihtoehto. Toinen, ja ehkä luultavampi verkonhallintaratkaisu on PBN, joka voi perustua LDAP-hakemistoihin, jolloin teknologian nimi on DEN (Directory Enabled Networking). Koska tässä ratkaisussa ei ole vianhallintaa, vikailmoituksiin tarvitaan SNMP (Simple Network Management Protocol). SNMP v3 tuskin on tulevaisuuden ratkaisu, koska siinä on paljon SNMP v1:n rajoituksia eikä esim. ohjelmistokonfiguraation hallintaa. Web-pohjaiset verkonhallintaratkaisut, kuten WBEM (Web-based Enterprice Management), ovat myös mahdollisia, joskin yksinkertainen SOAP (Simple Object Access Protocol) HTTP:n (Hypertext Transfer Protocol) päällä ratkaisu tuskin tulee tärkeäksi verkonhallinnassa koska se on olennaisesti standardoimaton ratkaisu. Samoin erilaiset agenttipohjaiset verkonhallintaratkaisut ovat täysin standardoi-mattomia.

Päävaihtoehtoja ovat luultavasti CORBA TMN, epästandardint CORBA-ratkaisut ja PBN/SNMP-yhdistelmä. Verkonhallinta tuskin päätyy yhteen standardiin tarkastel-tavana ajanjaksona. Verkonhallinta on kuitenkin olennainen osa tulevaisuuden verkkoa ja verkkotaistelun kannalta kiinnostava, koska sen avulla voi lamaannuttaa verkon. Verkonhallinnan osalta ei ole kehitetty varsinaisia tietoturvamalleja SNMP v3:a lukuunottamatta, vaan tietoturva perustuu pääosin esimerkiksi salausta käyttäviin kuljetusprotokolliin, kuten IPsec, TSL tai HTTPS.

5.2.6 Palvelut

Loppukäyttäjän palveluista ainakin seuraavia voidaan pitää myös 2020 skenaariossa tärkeinä palveluina: email, file transfer, WWW (World-Wide Web), VPN (Virtual Private Network, lähinnä MPLS VPN), VoIP, WAP (Wireless Application Protocol), eBusiness

(sähköinen kaupankäynti), mCommerce (kaupankäynti mobiilin avulla). Uusia palveluinnovaatioita on odotettavissa. Pääpaino uusissa palveluideoissa on toisaalta pienissä parannuksissa, jotka voidaan tehdä olemassaolevin tekniikoin, ja toisaalta videokuvan siirtoon perustuvissa tulevaisuuden palveluissa. Voitanee ajatella, että 2020 palvelut perustuvat paljolti reaaliaikaisen videokuvan siirtoon.

5.3. Tietoturvamekanismit

Tietoturva perustuun tietoturvapolitiikkaan ja tietoturvamekanismeihin. Kappale esittelee lyhyesti nykyiset tietoturvamekanismit yleisimmin käytetyistä alkaen.

5.3.1 Varmuuskopiot

Varmuuskopioilla yritetään suojautua tietojen tuhoamista vastaan. Varmuuskopiot tarvitaan paitsi tahallisten niin, myös vahingossa tapahtuvien tietojen tuhoutumisen estämiseksi. Menetelmä ei toimi hitaasti tietoja korruptoivia viruksia vastaan, koska ne tuhoavat myös varmuuskopiot, jotka olisivat vielä riittävän uusia käytettäväksi.

5.3.2 Käyttäjän tunnistaminen

Salasanaan perustuva käyttäjän tunnistaminen on käytössä lähes kaikissa tietokoneissa. Salasanan käytön tärkeimmät uhkakuvat ovat salasanan löytäminen paperille kirjoitettuna, salaamattoman tai heikosti salatun salasanan sniffaus, sanakirjahyökkäys jollain salasanakrakkausohjelmalla ja "social engineering". Näistä menetelmistä sniffaus on vähentynyt kytkentäisten lähiverkkojen yleistyessä, mutta langattomissa lähiverkoissa sniffaus on taas mahdollista mikäli salaus on murrettavissa, kuten WLAN:ssa. WLAN:in salaus paranee jatkossa, joten tämä ongelma ehkä poistuu. Toisaalta erilaisia ilmarajapinnan yli tehtäviä tunnistustoimenpiteitä on odotettavissa, ja niissä on aina joitakin heikkouksia. Esimerkiksi puolustusvoimien käyttämä ovenavausläpyskä on etäisluettavissa, vastaavanlaisia uhkia on tulevaisuudessa enemmän. Sanakirjahyökkäys toimii periaatteessa myös SSH (Secure Shell)-yhteyksillä, joskin sen tekeminen on hankalaa ja lopputulos saataa olla palvelun esto pikemminkin kuin salasanan löytyminen.

Salasanaa parempia menetelmiä on ehdotettu: sormenjälkitunnistus, silmän retinaan perustuva tunnistus ja PIN-koodi älykorttiin yhdistettynä. Näistä kahta ensimmäistä pidetään aiheetta turvallisina. Loppukäyttäjä jättää sormenjälkensä moneen paikkaan eikä ole mitään teknistä syytä siihen, etteiko sormenjäljen avulla voisi tehdä tunnistuslaitetta huiputtavan tunnisteen. Retinan varastaminen ei tarvitse olla silmän irroitaminen vaan yksinkertainen menetelmä, jossa käyttäjä huiputetaan tunnistamaan itsensä käyttäen laitetta joka tallentaa retinan kuvan. Jotta tämä olisi estetty, käyttäjän tulisi luottaa retinan lukijaan joten menetelmä soveltuu vain tiettyihin valvottuihin käyttötarkoituksiin. Sormenjäljen ja retinan ongelmana on myös se, että loppukäyttäjä ei voi vaihtaa niitä mikäli tieto joutuu hyökkääjän käsiin. On siis erittäin luultavaa, ettei tunnistus voi perustua näihin menetelmiin kuin erikoissovelluksissa. Loppukäyttäjän täytyy voida päästä järjestelmiin myös muualta, joten salasanat pysyvät myös käytössä. Tulevaisuuden menetelmät ovat luultavimmin salasana ja älykortti PIN-koodin kanssa. Yksi mahdollisuus on myös käyttäjän tunnistava vahvaa kryptologiaa käyttävä kortti ilman PIN-koodia, mutta se on varastettuna helpommin väärinkäytettävissä. On myös mahdollista jättää pois

paristo ja saada halpa laite joka ottaa energiansa antennilla, mutta silloin kryptologia on hankalaa. Erilaisia kaupallisia ratkaisuja on jo saatavissa. Salasana on ollut käytössä niin kauan, että sen turvallisuusongelmat ymmärretään. On tuskin mahdollista, että uudelleenkäytettävien salasanojen avulla voidaan parantaa tietoturvaa –käyttäjät tulevat jatkossakin valitsemaan heikkoja salasanoja, joilla hyökkääjät pääsevät järjestelmään. Kertakäyttösalasanalista on suhteellisen luotettava, mutta sen voi varastaa tai teeskennellä man-in-the-middle tyyppisesti kommunikaation toista osapuolta. Haaste-vastaus tyyppinen älykorttiin pohjautuva ratkaisu vaikuttaa parhaalta. Varkauden varalta on tietenkin tarpeen lisätä PIN-koodi. Menetelmässä on aukkoja: PIN-koodin voi saada selville kameralla tai lukemalla yhteydellä kulkevan datan, ja kortin voi varastaa. Social engineerin, siis käyttäjän huiputtaminen antamaan tunnisteensa hyökkääjälle, on mahdollinen sekä salasanoilla että älykortilla, joskin jälkimmäisessä ongelma on pienempi koska käyttäjän on annettava myös kortti. Käyttäjän tunnistaminen erillisellä tunnistamispalvelimella on eräissä suhteissa parempi ratkaisu kuin loppukäyttäjän tunnistaminen itse sovelluksessa. On todettava, ettei tunnistamisen suhteen ole tulossa tietoturvan suhteen oleellisia parannuksia jo käytettyihin menetelmiin. Käytetäävyyden osalta parannuksia saattaa tulla, esimerkiksi single-sign, vain yhden tunnisteen käyttö kymmenien salasanojen sijaan.

5.3.3 Pääsyoikeudet

Pääsyoikeuksilla rajoitetaan käyttäjien tekemiä toimintoja tietokoneessa. Tyypillisesti rajoitetaan pääsy vain tiettyihin hakemistoihin ja suojataan tietyt tiedostot kirjoittamis- tai lukemistoiminnnoilta. Pääsyoikeudet ovat käytössä olennaisesti kaikissa moderneissa tietokoneissa MS DOS-käyttöjärjestelmän jäätyä historiaan. Unixin pääsyoikeuksien ongelmana on, että käyttäjä käynnistäessään systeemikutsun useassa tapauksessa ajaa ohjelman, joka toimii suuremmilla oikeuksilla, esimerkiksi pääkäyttäjän oikeuksilla (root). Mikäli ohjelman saadaan käyttäytymään epätoivotulla tavalla, se voi antaa käyttäjälle pääkäyttäjäoikeudet. Tähän perustuu "local root exploit"-hyökkäys. Samanlaisen toiminnan voi joissakin tapauksissa tehdä myös suoraan verkosta ilman paikallisen käyttäjän oikeuksia, jollin puhutaan "remote root exploit"-hyökkäyksestä. Hyökkäystyypin voi estää vain mikäli: 1) käyttöjärjestelmä ei salli korkeamman pääsyoikeudella toimivien ohjelmien ajamista eikä sitä, että pääkäyttäjä antaa muille käyttäjille oikeuksia, 2) ohjelmat ovat virheettömiä eikä niissä ole eksploitin mahdollistavia aukkoja, 3) jokin muu kuin käyttöjärjestelmätason esto estää käyttäjää käynnistämästä ohjelmia, jotka toimivat pääkäyttäjän oikeuksilla. Toistaiseksi, ja ennustettavassa tulevaisuudessa 1) on mahdoton Unixissa koska se vaatisi koko käyttöjärjestelmän muuttamisen, 2) vaikuttaa mahdottomalta käytännössä, 3) on periaatteessa mahdollinen, mutta siihenkin jää käytännössä aukkoja. Näin siitäkin huolimatta, että Red Hat Linux-jakeluversio on ollut vajaan vuoden ilman tunnetuja eksploitteja ja 2) on ollut jonkin aikaa ehkä voimassa, mutta tämä ei vielä anna suurta varmuutta. Voidaan todeta, ettei eksploittien käyttöä voi täysin estää. Tästä seuraa, ettei nykyisen kaltaisilla pääsyoikeuksilla voi tietokoneen väärinkäyttöä kokonaan estää.

5.3.4 Virustarkistus

Virustarkistus perustuu yleensä viruksen sormenjäljen, siis viruskoodin palasen, löytämiseen saastuneesta ohjelmasta. Muitakin menetelmiä, kuten käyttäytymisen seuranta

ja arveluttavien komentojen etsimistä voidaan käyttää, mutta ne aiheuttavat vääriä hälytyksiä. Viruksia voidaan nykyään kehittää viruskehittimillä ja koska viruksen kehittäjä voi aina tarkistaa löytääkö virustarkistus sen, on sangen suoraviivaista kirjoittaa uusi virus, jota virustarkistus ei tunnista. Virukseen voi myös liitää erilaisia näppäriä menetelmiä koodin muuttamiseksi, virustarkistusohjelman sormenjälkitietokannan tuhoamiseksi, ym. Käytännössä virustarkistus siis toimii siten, että tarkistusohjelma tunnistaa tunnetut virukset ja uusi virustarkistusohjelma ladataan riittävän usein. Puolustusmenetelmässä on siis aukko: uudet hyvin tehdyt virukset pääsevät läpi ja joko aiheuttavat tuhoa (mikäli niin viruksen kirjoittaja on halunnut), tai ainakin koneiden irroittamisen verkosta. Jälkimmäinen puolustusmenetelmä aiheuttaa myös kuluja hukattuna työaikana. Viruksen poistaminen ja viruksen mahdollisesti tuhoamien tietojen palautus aiheuttaa myös kuluja.

5.3.5 Palomuuri

Palomuuri perustuu siihen, että verkkoelementti (reititin tai erillinen palomuuripalvelin) tarkastaa tietyt kentät tulevasta paketista ja tekee niiden perusteella päätöksen paketin päästämisestä läpi tai hylkäämisestä. Paketti voi olla periaatteessa millä hyvänsä kerroksista 2-7, mutta yleensä se on joko verkkokerrkosella (IP), kuljetuskerroksella (TCP (Transmission Control Protocol) tai UDP (User Datagram Protocol)) tai sovelluskerroksella. Kerroksen mukaisesti palomuurit jaotellaan pakettipalomuureihin (verkkokerros), piiritason palomuureihin (kuljetuskerros) ja sovellustason palomuureihin (sovelluskerros). Pakettipalomuurit edelleen jaetaa tilattomiin ja tilallisiin pakettipalomuureihin. Tilaton pakettipalomuuri tekee päätöksen jokaiselle paketille käyttämättä muista paketeista saatavaa tietoa, kun taas tilallinen pakettipalomuuri ymmärtää, että monta pakettia kuuluu samaan yhteyteen. Tilallinen pakettipalomuuri ymmärtää esimerkiksi, että FTP (File Transfer Protocol)-yhteydessä avataan kaksi yhteyttä (yhteyden muodostamiseen ja datalle), joilla on eri porttinumerot. Tilaton pakettipalomuuri voi käyttää vain IP-paketissa olevia salaamattomia kenttiä. (IP paketin kenttien salaaminen tulee kyseeseen IPsec (IP Security Protocol) protokollassa.) Käsiteltävät kentät ovat yleensä IP osoitteet ja TCP/UDP porttinumerit.

Palomuurin ongelma puolustusmenetelmässä johtuu siitä, että palomuuriin voi avata reikiä koska palomuuri aina sallii toiseen suuntaan yhteyden oton jollain protokollalla, muutenhan palomuurin voisi korvata irroitamalla koneen kokonaan verkosta. Reiän voi avata mikäli palomuurin takana olevassa suojatussa verkossa oleva käyttäjä voi vastaanottaa sähköpostia keneltä hyvänsä ja itse ottaa yhteyden mihin hyvänsä WWW-palvelimeen suojatun verkon ulkopuolella. Tämä tilanne on yleensä voimassa yhteiskunnassa koska halutaan sähköpostin saavuttavan kaikki ja WWW:n olevan kaikkien saavutettavissa. Lähettämällä loppukäyttäjälle haittaohjelman sisältävän viestin hyökkääjä saa asennettua käyttäjän koneelle ohjelman, joka esim. HTTP-protokollaa käyttäen muodostaa käyttäjän koneen aloitteesta piilokanavan hyökkääjän ja käyttäjän välille. Tällöin hyökkääjä voi käyttäjän koneelta, siis palomuurin takaa, jatkaa toimintaansa mihin hyvänsä suojatussa verkossa olevaan koneeseen. Mikäli piilokanava on salattu, palomuuri ei voi mitenkään tietää mitä dataa siinä kulkee.

Vaikka sähköpostilla virusten tai troijalaisten saaminen olisi estetty, palomuurin ongelma ei poistu. Oletetaan esimerkiksi, että palomuuri salliin vain ulos menevän HTTPS yhteyden, kuten turvallisissa verkoissa usein tehdään. Hyökkääjä voi selvittää mille WWW-

sivulle laillinen käyttäjä menee, hakkeroda nimipalvelimen julkisessa, siis sangen turvattomassa, Internetissa ja ohjata käyttäjän omalle sivulleen, jonne on laadittu alkuperäisen sivun kaltainen sivu. Jos yhteys on HTTPS, tulee vielä ratkaista tunnistuksen huiputus. Se voi perustua huolimattomaan käyttäjään, joka uskoo sivun olevan oikea koska se näyttää oikealta, eikä tarkista julkisen avaimen tunnistusta, tai voidaan yrittää huiputtaa käyttäjää uskomaan, että julkinen avain on vaihdettu ja annetaan uusi avain, joka on hyökkääjän julkinen avain. Tämän jälkeen HTTPS vastaus voi tuoda turvallisen verkon sisälle mitä hyvänsä sisältöä, esimerkiksi takaoven. Hyökkääjän täytyy vielä huiputtaa käyttäjä käynnistämään takaoven. Sopivasti suunnitellen tällainen hyökkäys on toteutettavissa. Se ei vaadi olennaisesti mitään tietoa käyttäjän järjestelmistä vaan perustuu heikkoon turvallisuusmalliin Internetin palveluissa.

5.3.6 DMZ, dead zone

Demilitarisoitu vyöhyke (DMZ) on kahden tai useamman palomuurin välissä oleva alue, jonka turvallisuus on turvallisen verkon ja julkisen Internetin turvallisuuden välillä. Kuollut alue on DMZ-alue, joka on luotu muuttamalla protokolla IP:stä joksikin muuksi, esimerkiksi Novelin IPX-protokollaksi. Kuolleella alueella voidaan vaikeuttaa esimerkiksi ICMP:n (Internet Control Message Protocol) avulla tehtäviä hyökkäyksiä ja tiedusteluita. Korkeamman tason protokollat tunneloidaan kuolleen alueen yli, joten niihin menetelmä ei toimi.

5.3.7 Hiekkalaatikko

Hiekkalaatikko on Javan käyttämä turvallisuusmekanismi ja pääturval-lisuusmenetelmä joka tekee mahdolliseksi WWW sivujen applettien käyttämisen. Verkosta saatava koodi ajetaan rajoitetussa ympäristossä, jossa se ei pääse tekemään mitään vaarallista. Menetelmän haittana on, että hiekkalaatikossa ajettava koodi ei pääse tekemään toimintoja, joita ehkä toivottaisiin: ympäristö rajoittaa koodin olennaisesti grafiikan näyttämiseen ja tietojen keräämiseen käyttäjältä. Javan hiekkalaatikkomalli on tunnetuin hiekkalaatikkomalli. Se sisältää seuraavat osat: Java tavukoodin verifikaattori – tarkistaa, ettei tavukoodiin ole käsin asetettu esimerkiksi osoittimia hiekkalaatikon ulkopuolelle eikä muita vaarallisia komentoja, luokkalataaja - asettaa verkosta ladatun koodin omaan osoiteavaruuteensa josta se ei pääse tekemään tuhoja, turvallisuusmanageri – hallitsee turvallisuutta esimerkiksi allekirjoitetujen applettien pääsyoikeuksia.

Hiekkalaatikko, jos sellainen on virheettä toteutettu, on hyvä turvallisuusmenetelmä, mutta liian rajoitettu koska liikkuva koodi ei voi toteuttaa kaikkia komentoja. On ilmeistä, että tulevaisuudessa liikkuvalta koodilta odotetaan paljon suurempaa toiminallisuutta kuin hiekkalaatikkomalli sallii.

5.3.8 Tiedon salaus

Suuri joukko protokollia käyttää salausta tiedon yksityisyyden ja muuttumat-tomuuden varmistamiseksi. Niillä voi estää tiedon salakuuntelun (sniffauksen) sekä TCP-yhteyden kaappauksen.

TLS (Transport Layer Security, myös tunnettu nimellä SSL, Secure Socket Layer)

Salattu TCP yhteys. Nykyiset TLS-toteutukset ovat sangen hyviä, mutta ongelmia liittyy julkisen avaimen varmenteiden käyttöön. TLS salaa tiedon sangen hyvällä symmetrisellä salausalgoritmilla, mutta istuntoavaimen vaihdossa käytetään julkisen avaimen menetelmää, joka luottaa siihen, että sertifikaatti eli varmennin tarkistetaan. Useat TLS toteutukset eivät todellisuudessa kunnolla tarkista varmennetta. Itse asiassa varmenteiden käyttö tiedonsiirrossa tuntemattomalle osapuolelle vaatii julkisen PKI ratkaisun, jota ei vielä ole laajasti käytössä.

HTTPS

Salattu HTTP protokolla. Turvallisuuden osalta HTTPS on kuten TLS.

SSH

Salattu Telnet ja FTP yhteys (SCP). Turvallisuus on kuten TLS.ssä, mutta lisäksi uhkana on sanakirjahyökkäys.

IPsec

IPsec on noussut tärkeäksi ratkaisuksi, jossa IP-verkossa kulkeva tieto salataan IP kerroksella. Ratkaisun ongelmana on se, että IPsec paketit ovat sangen suuria ja kapasitettia hukkaantuu. On todennäköistä, että IPsec ei tule operaattorien näkökulmasta suosituksi ratkaisuksi vaan turvallisuus perustuu jatkossa siihen, että data kulkee operaattorin verkossa johon pääsy on hankalaa. Ratkaisu on siis samanlainen kuin perinteisessä puhelinverkossa. Erityisen luultava tämä menettely on tulevaisuudessa IP puheessa. Jos VoIP liikenne salataan IPsec:n avulla, niin puhepakettien hyötydatan osuus koko paketin koosta tulee erittäin pieneksi. Yritykset saattavat kuitenkin käyttää IPsec:iä operaattorilta tilatun MPLS VPN:n päällä, varsinkin kun operaattoreiden verkkoa ei enää jatkossa voi ehkä pitää tietoturvallisena. Operaattorin verkon teitoturvahan varmistetaan vain lainsäädännöllä, verkossa kuljetetun tiedon lukeminen on rikos.

PGP (Pretty Good Privacy)

Salattu sähköpostiohjelma PGP käyttää vahvaa salausta mutta ilman PKI.ta. PGP:n tapa hallita sertifikatteja on menetelmän heikkous: käyttäjät muodostavat keskenään luottamuksen verkon. Hyökkääjälle ei liene vaikeaa päästä luottamuksen verkkoon uskottelemalla olevansa luotettava henkilö. Toinen heikkous on PGP.n tapa säilyttää avaimet avainrenkaassa, joka on suojattu tietokoneen pääsyoikeuksilla. Pääsyoikeuk-sissa on usein aukkoja. Menetelmän pääongelma on se, ettei se mahdollista globaalia sähköpostia. Kaikkien tulisi voida lähettää postia kaikille, mutta silloin kaikkien tulisi olla luotettuja, jolloin hakkereita ei lainkaan olisi. Vain julkinen PKI mahdollistaa salatun sähköpostin tuntemattomalle vastaanottajalle.

Avainten vaihto protokollat

Istuntoavaimen vaihto tai luonti kuuluu olennaisena osana salausta käyttäviin protokolliin. Avainten vaihdon voi myös ratkaista erillisellä yleiskäyttöisellä avainten vaihtoprotokollalla, kuten Diffie-Hellan key exchange. IPsec:in käyttämä IKE (Internet Key Exchange) lienee tunnetuin avainten vaihtoprotokolla. IKE:een liittyvät saman ongelmat kuin muihinkin salaisen avaimen setrifikaatteihin perustuviin menetelmiin, siis jokin man-in-the-middle hyökkäys tai väärän julkisen avaimen antaminen, jossa hyökkääjä teeskentelee olevansa jokin muu.

5.3.9 PKI (Public Key Infrastructure)

Sertifikaatit eli varmenteet ovat vahvassa tunnistamisessa käytettyjä tietorakenteita, jossa on sähköisesti allekirjoitettu käyttäjän julkinen avain. PKI on tietokanta, jossa varmenteita säilytetään. Yleensä kyseessä on LDAP tai X.500 tietokanta. PKI ei ole yleistynyt käytössä, kaupallisesti tarjottuja PKI-palveluita on pidety liian kalliina ja PKI:ta käyttäviä ratkaisuja liian hitaina, kuten sähköisen kaupankäynnin luottokorttiostosprotokollaa SET (Secure Electronic Transactions). Varmenteiden käyttöön liittyy pieniä uhkia, jotka yleensä ovat muutenkin olemassa: esimerkiksi paljastuneita yksityisiä avaimia vastaavien julkisten avainten poisto tapahtuu periodisesti (PKI:n päivitäminen mielivaltaisena aikana on myös turvatonta, koska silloin ei tiedä onko päivitys oikea). Jos hukkaa yksityisen avaimensa niin järjestelmään jää tietty aikaikkuna jolloin hyökkääjä voi käyttää julkista avainta. Tilanne on sama kuin jos hukkaa luottokorttinsa ja puhelimensa eikä pääse ilmoittamaan luottokunnalle, joten tällainen uhka on muuallakin olemassa. Toinen absurdi mutta todellinen uhka PKI:ssa on se mahdollisuus, että siirrytään turvallisuudeltaan heikkoihin PKI:tä korvaaviin menetelmiin. On esimerkiksi esitetty, että IP osoite (esim. ad-hoc osoite ad-hoc IP-verkoissa) voitaisiin sitoa julkiseen avaimeen, jolloin julkista avainta ei tarvitse hakea mistään PKI tietokannasta. Näiden ehdotusten ongelma on, ettei sellainen IP-osoite ole muistettavissa, joten se on haetava jostain varastosta, jossa siis voisi yhtä hyvin olla myös julkinen avain. Edelleen, on aina vaarallista sitoa julkinen avain mihinkään tietoon jota ei halua muuttaa sen vuoksi, että salainen avain on aina mahdollista hukata jolloin julkinen avain on vaihdettava.

PKI on tarpeellinen lisä sähköisen kaupankäynnin mahdollistamiseksi. Mobiili-kaupankäyntiin kehitellään WPKI (Wireless PKI) ratkaisua. PKI on erittäin todennäköisesti laajamittaisesti käytössä 2020 ja varmenteisiin kohdistuvat uhat paljolti torjuttu tai ainakin niiden riskit on hallittu. Riskien hallitseminen tarkoittaa, että mahdollisen väärinkäytön korvaa jokin riskin ottava taho.

5.3.10 IDS (Intruder Detection System)

Intruder Detection System, hyökkääjän havaitsemismekanismi, on turvallisuusmallin uusin osa tietoverkkojen turvallisuusmallia. IDS nimellä kulkee erilaisia ratkaisuja, jotka voidaan karkeasti jakaa Host-IDS ja Network IDS järjestelmiin. Host-IDS perustuu hyökkäyksen havaitseviin ohjelmistoihin tietoverkon koneissa. Esimerkkinä Host-IDS:stä on LIDS (Linux IDS) ohjelmisto, joka yrittää parantaa turvallisuutta estämällä pääkäyttäjä toteuttamasta vaarallisia komentoja ilman erillistä salasanaa. Network IDS (NIDS) on IDS järjestelmä, joka lukee kaiken datan, joka kulkee sen kautta, ja tekee siitä päätelmiä

onko kyseessä hyökkäys. Esimerkkinä NIDS järjestelmistä on ilmaisohjelmisto Snort. NIDS ei yleensä itse reagoi hyökkäykseen vaan tallentaa hälytyksen lokitietoihin. NIDS:n ongelmana on suuri väärien hälytysten määrä. Toinen ongelma on se, että lokitietoja tulee säilyttää mahdollista oikeudenkäyntiä varten ja koska lokitietoa muodostuu valtavasti, sitä on osattava karsia siten, että hyökkäykset jäävät säilöttävään dataan. Hyökkääjä voi yrittää lamaannuttaa NIDS järjestelmän tekemällä suuren määrän valehyökkäyksiä.

Tunnistamisvarmuus IDS:ssä ei ole kovin suuri, vain noin 70% hyökkäyksistä havaitaan. Tunnistaminen perustuu yleensä hyökkäyksen sormenjälkeen, eli sille tunnusomaiseen bittikuvioon hyökkääjän lähettämissä paketeissa. Tällainen menetelmä ei suojaa uusilta hyökkäystyypeiltä ja olisi tietenkin parempi estää tunnetut hyökkäykset korjaamalla sovellutukset sen sijaan, että tunnistetaan hyökkäys. On kokeiltu erilaisia menetelmiä tunnistaa poikkeava käyttäytyminen ja näin havaita myös uudet hyökkäykset, mutta toistaiseksi tällaiset menetelmät tekevät liian paljon vääriä hälytyksiä.

5.3.11 Käyttäjän tunnistamispalvelin

Käyttäjän tunnistaminen voidaan suorittaa myös erillisellä tunnistamispalvelimella sen sijaan,että palvelin, johon yhteys otetaan myös suorittaa tunnistamisen. Menetelmän etuna on, että tunnistamispalvelin on helpompi tehdä turvalliseksi. Haittapuolena on se, että tunnistamispalvelin on haavoittuva solmupiste.

AAA (Authentication Authorization and Accounting) palvelin

AAA palvelimia, kuten RADIUS ja DIAMETER, tullaan käyttämään tiedonsiirtopalvelussa laskutuksen osana. RADIUS on käytössä, mutta tarkoitettu vain dial-up käyttäjille, DIAMETER on toistaiseksi epästabiili RFC, mutta sitä jo nyt tuetaan. AAA on tulevaisuuden IP-pohjaisen tiedonsiirtoverkon (NGN Next Generation Network) olennainen osa ja tulee käyttöön nopeasti. Se saattaa olla turvallisuusmallin osa vielä vuonna 2020.

Kerberos – Active Directory

Kerberos on jo vanha käyttäjän tunnistamispalvelu, mutta vientirajoituksista johtuen sen käyttö rajoittui lähinnä USA:aan. Kerberos palvelin antaa loppukäyttäjille tikettejä, joilla he pääsevät verkon palvelimiin. Kerberokseen voidaan kohdistaa useita hyökkäyksiä, esimerkiksi verkon ajan muuttaminen. Windows NT and Win 2000 sisältävät Kerberos autentikoinnin osana Active Directory mallia, joten protokolla on edelleen ajankohtainen. Protokolla tuskin on enää käytössä 2020, mutta joitakin perusajatuksia varmaan edelleen sovelletaan.

5.3.12 NAT (Network Address Translation)

IPv4:n osoiteavaruus olisi jo loppunut, ellei olisi siirrytty NAT:n käyttöön. NAT on myös pääsyy siihen, ettei painetta IPv6:n käyttöön juuri ole. NAT on tietyssä mielessä tietoturvamenetelmä, koska se vaikeuttaa IP-osoitteen väärentämistä ja vaikeuttaa, muttei estä, NAT:in takana olevien koneiden löytämistä. NAT todennäköisesti ei estä NAT:n takana olevien koneiden löytämistä koska koneet voidaan tunnistaa eräänlaisista verk-

kosormenjälistä: kukin kone vastaa hieman eri tavalla. (Nämä sormenjäljet eivät ole fyysisen tason sormenjälkiä, kuten signaalitasoja joita radiotiellä voi käyttää koska sellaiset häviävät ensimmäisessä toistimessa, vaan ikkunakokoja, nopeuksia, optioita, bannereita ym.) NAT ei ole varsinainen turvallisuusmekanismi ja IPv4 lienee historiaa 2020.

5.3.13 Allekirjoitettu koodi

Koodista muodostetaan hash-tiiviste, joka salataan yksityisellä avaimella. Näin saadun allekirjoituksen voi kuka hyvänsä tarkistaa. Menetelmä on käytössä esimerkiksi liikkuvassa koodissa Javan allekirjoitetuissa appleteissa ja ActiveX:ssä, sekä paikallisesti ohjelmien muuttumattomuuden varmistamisessa. Menetelmän ongemana on, ettei allekirjoitus takaa muuta kuin että allekirjoittaja uskoi koodin olevan turvallista, mutta sitähän hän ei voi tietää. Koodi voi käyttäytyä eri tavalla eri ympäristossä ja koodin varsinainen kirjoittaja on voinut asettaa siihen haitallisia osia jotka laukeavat vasta kohdekoneessa. On myös epäselvää voiko allekirjoittaneeseen tahoon todella luottaa. Vain allekirjoitusta käyttäviä menetelmiä, kuten Active X ei pidetä riittävän turvallisina. Allekirjoitetu koodi on harvoja tunnettuja menetelmiä liikkuvan koodin turvallisuuden parantamiseksi ja oletettavasti pysyy käytössä vielä 2020.

5.3.14 Turvallisuusskanneri

Turvallisuusskannereita käytetään tarkistamaan tietokoneen tai tietokoneverkon turvallisuus. Skanneri kerää tietoa verkon koneista ja osa skannereista yrittää tehdä tunnettuja hyökkäyksiä. Skanneri on sekä hakkerin työkalu että puolustuksen menetelmä järjestelmän turvallisuuden tarkistamiseksi. Turvallisuusskanneri tarkistaa vain tunnettuja hyökkäyksiä, joten se ei takaa turvallisuutta.

5.2.15 Virhelistat ja CERTit

WWW:ssä julkaistaan useita listoja ohjelmistojen tietoturva-aukoista eli bugeista. Usein bugiin liittyen esitetään toimiva hyökkäys ja annetaan sille jopa hyökkäyskoodi (exploit script). Menetelmässä yritetään vähentää toteutusten virheitä olennaisesti pakottamalla ohjelmistovalmistajat korjaamaan virheensä ja loppukäyttäjät päivittämään ohjelmaversionsa. Haittapuolena on se, että hyökkääjä voi yksinkertaisesti selata listoissa olevia uusia bugeja, poimia valmiin hyökkäysskriptin ja käyttää sitä sellaiseen koneeseen, jonka käyttäjä ei viitsi, ehdi tai tiedä tehdä päivityksiä. Erityisesti kotikäyttäjissä on paljon niitä, joilla ei ole tietoa tai kiinnostusta tietoturvapäivityksiin, joten hyökkääjä löytää helposti koneita joihin hän pääsee hakkeroimaan, vaikka hyökkääjällä ei olisi mitään erityisosaamista tietoturvasta. Bugilistojen yhteydessä tai hakkerisivuilta hyökkääjä saa ilmaiseksi vaikuttavan valikoiman hyökkäystyökaluja. Bugilistoissa on toisaalta periaatteellinen mahdollisuus rekisteröidä listoilla kävijät, jolloin hakkereiden löytäminen voisi helpottua.

Computer Emergency Response Team (CERT) on ryhmä tietoturva-asiantuntijoita, jotka seuraavat verkossa tapahtuvia hyökkäyksiä ja ryhtyvät vastatoimiin. Menetelmä on varmasti hyödyllinen ja toiminta laajenee vuoteen 2020 menenssä. On luultavaa että hakkereita yritetään vieläkin aktiivisemmin löytää ja ehkä jopa ehkäistä toimintaa ennalta. Terrorismiuhka johtanee tähän.

Avoimuuden periaate tietoturvassa on voimakas ja bugien julkistaminen epäilemättä jatkuu. Johtaako se koodin virheettömyyteen misään aikataulussa on epäselvää. Julkisuus toimii esimerkiksi salausalgoritmin aukkojen löytämisessä. Koodin suhteen tilanne on toinen. Koodia on niin paljon ja uutta koodia kehitetään niin nopeasti, ettei tunnettujen virheiden korjaminen luultavasti koskaan anna virheetöntä ohjelmistoa.

5.3.16 Hunajapurkki

Menetelmässä asetetaan verkkoon houkutuslinnuksi kone, johon tunkeutuva hakkeri ei pääse tekemään mitään vaarallista mutta hänen toimintojaan voidaan seurata. Hunajapurkkien ja houkutuslintujen osalta eettiset kysymykset rajoittavat käyttöä: on hieman epäselvää milloin kyseessä on rikokseen yllyttäminen.

5.3.17 Tiger team

Tässä menetelmässä joukko asiantuntevia tietoturvaeksperttejä yrittää hakkeoida järjestelmään laillisesti. Menetelmä voi paljastaa aukkoja muttei takaa turvallisuutta. Eräänä versiona on asettaa hakkerointihaasteita tietoturvakurssin opiskelijoille. Tällaista haastetta sopivalla palkinnolla on ajateltu kokeiltavan eräällä TKK:n hakkerikurssilla 2003. Toistaiseksi menetelmästä ei ole riittävästi kokemusta päätelmien tekemiseksi.

Lopuksi esitetään joitakin kokeiluasteella olevia turvallisuusmekanismeja. Lista ei ole kattava.

5.3.18 PCC (Proof Carrying Code)

Liikkuva koodi sisältää todistuksen oikeellisuudestaan. Vastaanottava solmu voi tarkistaa todistuksen. Kokeellinen menetelmä, jota on ehdotettu esimerkiksi liikkuville agenteille.

5.3.19 Palvelunestohyökkäyksen paikallistamienn

On esitetty menetelmää, jossa reititin kirjoittaa muutaman bitin tietoa läpikulkeviin IP-paketeihin. Mikäli paketteja tulee riittävästi samasta osoitteesta, niin tästä tiedosta saadaan paketin reitti selville. Menetelmällä voidaan paikallistaa palvelunesto-hyökkäyksen tekijä vaikka hän säännönmukaisesti väärentääkin lähettäjän osoitteen IP-paketeissa. Menetelmä ei ole vielä käytössä ja ratkaisua voidaan pitää vain yhtenä ideana.

5.3.20 Agenttipohjainen puolustus

Keskenään keskustelevilla agentti-tekniikkaan perustuvilla puolustusmenetelmillä on saatu hyviä kokemuksia. Konkreettisena esimerkkinä on liikkuvilla agenteilla toetutettu hajautetun palvelunestohyökkäyksen esto: liikkuvat agentit kulkevat lähelle hyökkääjiä (hyökkääjän paketeissa saa olla väärä lähettäjän osoite) ja ohjelmoivat reitittimet estämään tietystä osoitteesta tulevat paketit. Toistaiseksi liikkuvien agenttien ja aktiiviverkkojen turvallisuusongelmat ovat sitä luokkaa, ettei niitä uskalleta käyttää.

5.3.21 Koodin validointi ja todistaminen oikeaksi

On kieliä, joilla voidaan löytää virheitä koodista. SDL kielisiin määritelmiin on kehitetty validaattoreita. Koodin todistaminen oikeaksi on mahdollista eräissä kielissä (Prolog, Z, ObjectZ). Näistä Z ja ObjectZ ovat laajimmin käytössä, mutta käyttö on erittäin pientä.

5.3.22 Muita

Muita tietoturvamekanismeja on sangen paljon, mutta ne eivät ole laajassa käytössä. Voidaan ehkä lisätä langattoman yhteyden taajuushyppelu ja muut hajaspektri-menetelmät, jossa pseudosatunnaisjonolla on tiettyjä turvallisuutta parantavia ominaisuuksia. Hajaspektritekniikkassa satunnaislukugeneraattori ei sinänsä ole tietoturvamekanismi, vaan häirinnän estomekanismi, joten käytetyt satunnaisluku-generaattorit eivät usein ole kryptologisesti vahvoja.

5.4 Nykyisten puolustusmenetelmien puuteet

Hyökkäyksiltä kokonaan suojautuminen esitetyissä skenaarioissa ei ole mahdollista, vaikka tietoturvaa voidaankin parantaa ja tehdä hyökkäykset vaikeammiksi. Seuraavat tietoverkon uhat eivät ole kokonaan estettävissä nykyisessä IP-verkossa:

5.4.1 Haittakoodi

Virusten, matojen, troijalaisten ja muun haittakoodin muodostama uhka ei ratkea virustorjuntaohjelmilla. Uusien ja tuntemattomien virusten tunnistaminen on vaikea. Ongelma on se, että sähköposti ja muut tieton siirtämistavat mahdollistavat mielivaltaisen koodin siirtämisen. Uusien virusten havaitsemiseen on olemassa eräitä jo käytettyjä keinoja: käyttäytymisen seuraaminen, protokolla-analyysi ja hiekkalaatikko.

Käyttäytymisen seuraamisessa ajetaan tuntematon ohjelma tai avataan mahdollisesti haittakoodia sisältävä sähköposti rajoitetussa hiekkalatikkoympäristössä. Jos koodi ei jossain valitussa ajassa näytä tekevän mitään vaarallista päätellään, ettei haittakoodia ole. Looginen ongelma menetelmässä on se, että haittakoodi voi käynnistyä loogisella pommilla esimerkiksi jonkin pitkän ajan päästä. Käyttäymisen seurannassa on oltava jokin suhteellisen lyhyt aika, jotta tutkittava ohjelma tai sähköposti voidaan todeta turvalliseksi niin nopeasti, että se on hyödyllinen käyttötarkoitukseensa.

Protokolla-analyysilla olisi voitu havaita esimerkiksi Nimda mato. Eräissä madoissa ja viruksissa käytetään hyväksi tiedonsiirtoprotokollan virheitä ja lähetetään väärin muotoiltuja paketteja. Protokolla-analyysi havaitsee tällaisen. Kaikki virukset ja madot eivät hyödynnä tällaisia virheitä, joten menetelmä ei aina toimi. Toisaalta protokolla-analyysi soveltuisi paremmin vastaanottavalle protokolla-automaatille, jotta siinä ei olisi virheitä joita voidaan käyttää hyväksi. Tämä menetelmä todennäköisesti poistuu ja korvataan protokolla-analyysin ja validoinnin käyttämisella protokollasuunnittelussa ja toteutuksessa. Menetelmään kuitenkin jää helposti aukkoja koska kaikkien mahdollisten kombinaatioiden läpikäyminen ei ole ainakaan vielä mahdollista vähääkään mutkikkaammalle protokollalle.

Hunajapurkkimenetelmä uusien virusten ja matojen löytämiseksi perustuu siihen, että haittakoodi ei voi olla niin älykäs, että se pystyisi tunnistamaan hunajapurkin vaan yrittää saastuttaa myös hunajapurkin. Logiikka hunajapurkissa on, ettei sinne kenelläkään tulisi olla asiaa, joten sinne tullut uusi ohjelma voidaan havaita. Hunajapurkkia on pidetty rikokseen houkuttelemisena, joten menetelmä ei ole suosittu. Kuitenkin, jos hunajapurkki on turvallisen verkon sisällä, voidaan argumentoida että turvallisen verkon sisään päästäkseen hyökkääjä on jo tehnyt rikoksen. On selvää, ettei uusi virus aina kulkeudu ajoissa hunajapurkkiin tai tule siellä esille.

Näiden menetelmien antamaa suojaa ei voi pitää riittävänä. Liikkuvan laillisen koodin käyttö on kasvamassa ja samalla haittakoodin uhka kasvaa.

5.4.2 Palvelunestohyökkäys

IP verkko antaa loppukäyttäjälle mahdollisuuden generoida paljon liikennettä, toisin kuin esimerkiksi puhelinverkko, jossa yksi puhelin synnyttää vain 64 kbps dataa. Tästä seuraa, että suhteellisen pieni määrä käyttäjiä voi synnyttää niin paljon liikennettä, että verkkoelementti, tai jopa kokonainen aliverkko, saadaan tukkoon. Ongelma on looginen, ilman liikenteen rajoitusta rajallinen kapasiteetti voidaan aina ylittää. Yhden lähteen generoiman Internetin liikenteen rajoittaminen niin pienelle tasolle ettei tällaista uhkaa olisi ei ole toivottavaa, koska verkon käyttötarkoitus kärsisi liikaa. Näin ollen, nykyisessä Internetissä hajautettua palvelunestohyökkäystä ei yleisessä mielessä voi estää. On toki mahdollista parantaa nykyisiä menetelmiä, esimerkiksi jos havaitaan useassa solmupisteessä korreloitu datavuo johonkin osoitteeseen, niin tällainen vuo voidaan siirtää QoS IP:ssä matalammalle palvelu-luokalle. Vastaavia menetelmiä voidaan helposti keksiä ja ne purevat tiettyihin tyyppeihin palvelunestohyökkäyksiä. Ongelman ratkaisu on kuitenkin lähinnä looginen mahdottomuus nykyisellä palvelumallilla, joten mikään korjausmenetelmä ei toimine kaikkia hyökkäystyyppejä vastaan.

5.4.3 Datan hidas korruptointi

Virus, joka muuttaa dataa hitaasti ja sieltä täältä voi sangen kauan toimia huomamatta tietokoneessa. Se saattaa onnistua korruptoimaan varmuuskopiot, jolloin dataa ei voida palauttaa helpolla tavalla. Koska uusien virusten pääsemistä virustarkistuksen läpi ei voida kokonaan estää, dataa hitaasti korruptoivia viruksia ei voi estää. Täsmäviruskäsite on hieman epäselvä, mutta soveltuisi ehkä hitaasti dataa korruptoiviin viruksiin. Viruksen on luultavasti pakko levitä niin nopeasti kuin se pystyy, koska muuten se ehkä ei leviä lainkaan. Tässä mielessä virus joka leviää vain joihinkin koneisiin ei ole mielekäs. Sen sijaan viruksen toiminta voi olla koneriippuva. Jos virus on hitaasti dataa korruptoiva ja suunniteltu pysymään kauan salassa, se voi yrittää tuhota vain tietyn verkon koneiden tietoja, vaikka leviääkin laajalti leviämisen varmistamiseksi. Tällaista virusta voi hyvin kutsua täsmäviruk-seksi.

5.4.4 Ohjelmistojen virheiden käyttö

Ohjelmistovirheet mahdollistavat hakkeroinnin, esimerkiksi siirtymien pääkäyttäjäksi eksploittien avulla. On ajateltu, että samoin kuin kryptoalgoritmeilla, julkisuus-periaate johtaisi virheiden määrän pienenemiseen ja lopulta niiden poistumiseen. Virheiden jul-

kistamien toki johtaa havaittujen virheiden korjaamiseen, mutta korjauksissa on usein muita virheitä. Ongelma ohjelmistoissa on se, että koodia on erittäin paljon ja uutta kehitetään koko ajan. Lisäksi koodia ei voi poistaa käytöstä heti kun virhe havaitaan, vaan virhe on yritettävä korjata nopealla tavalla, ja koodin nopea muuttelu usein aiheuttaa erilaisia sivuvaikutuksia. Ei ole mitään syytä uskoa, että julkisuusperiaate virheiden osalta, sen enempää kuin täysin julkinen koodikaan, johtaisi virheiden katoamiseen.

5.5. Puolustautuminen nykyisillä menetelmillä

Tässä osassa käsitellään verkkohyökkäyksiltä puolustautumista yleisesti, ottamatta kantaa kappaleen 1 skenaarioihin. Puolustautuminen perustuu verkon rakentamiseen mahdollisimman turvalliseksi esitetyillä turvallisuusmekanismeilla ja turvallisuus-politiikan käyttöön. Turvallisuuspolitiikalla pyritään ohjeistamaan yrityksen työntekijöiden toimintaa siten, ettei turvallisuusriskejä syntyisi. Käytännössä ohjeistetaan salasanojen käyttöä ja vaihtamista, salaisten tietojen sälyttämistä sekä uusien henkilöiden palkkaamisessa huomioonotettavia turvallisuusnäkökulmia. Tietoturvapolitiikan antama turvallisuus toiminee hyvin (mikäli toimii) lähinnä vain puolustusvoimien kaltaisessa instituutiossa, jossa pääsy luokiteltuihin tietoihin voidaan rajata henkilöille, jotka ovat sisäistäneet tietoturvapolitiikan. Yritysmaail-massa, esimerkiksi high-tech yrityksissä tilanne on vaikeampi: yritykselle tärkeää ja salassapidettävää tietoa tuottavat henkilöt eivät ole useinkaan siinä määrin sisäistäneet tietoturvapolitiikkaa, että he riittävästi ottaisivat huomioon tietoturva-asiat.

Hyökkäyksen tapahtuessa se pyritään havaitsemaan, mutta vain pieni osa hyökkäyksistä todellisuudessa havaitaan. Hyökkääjän toimintaa tarkastellaan ja pyritään keräämään riittävästi tietoa mahdollista syytettä varten, samalla suojautuen hyökkäyksen vaikutuksilta. Tämä voi tapahtua esimerkiksi ohjaamalla hyökkääjä hunajapurkkiin. Puolustaja voi yrittää paikallistaa hyökkääjän selvittämällä mistä osoitteesta hyökkäys tulee. Koska hyökkääjä harvemmin käyttää omaa konettaan vaan tekee hyökkäyksen monen koneen kautta, paikallistaminen vaatii yhteistoimintaa yleensä usean maan ylläpitohenkilökunnan kanssa. Paikallistaminen yleensä päätyy siihen, että hyökkääjän jälkiä voidaan seurata johonkin vaiheeseen, mutta vaikka hänet pystyttäisiinkin tunnistaman, häntä ei saada oikeuteen koska hakkerointi tai virusten lähettäminen ei ole rikos kaikissa maissa, ainakaan jos kohde on toisessa maassa.

Ohjelmistoissa olevia virheitä tai piirteitä hyväksikäyttäen tehdyltä hyökkäykseltä pyritään suojautumaan julkistamalla hyökkäys, jolloin valmistajat pakotetaan korjaamaan virhe tai piirre. Menetelmä toimii, mikäli ylläpitohenkilökunta ehtii seuraamaan tietoturvailmoituksia ja tekemään vaadittavat päivitykset. On hyvin epäluultavaa, että yksityiskäyttäjät tai kaikki pienet yritykset ehtisivät näitä päivityksiä tekemään, joten menetelmän haittana on, että Internetistä löytyy paljon kohteita joihin julkistetut hyökkäykset toimivat.

Nykyistä puolustautumismenetelmää on kuvattu kilpajuoksuksi hyökkääjän ja puolustajan välillä. Asejärjestelmien osalta kehitys on aina eräänlaista kilpajuoksua, mutta verkkohyökkäyksien osalta puolustaja on selvästi huonommassa asemassa. Puolustaja odottaa hyökkäyksiä, muttei itse ryhdy vastaaviin hyökkäystoimenpiteisiin. Mahdolliset rangaistukset kiinni jääneelle hyökkääjälle ovat kovat, mutta kiinni-jäämisriski on pieni.

Eräs ongelma verkkotaistelun käsittelemisessä on, ettei riskien mallintamiseen ole hyviä menetelmiä, jolloin vaikutuksen arvoiminen on vaikeaa. Verkkotaistelua on usein esitetty mallinnetavaksi riskiteorian menetelmillä. Tällöin ajatellaan, että on tietty todennäköisyys, että tietyn tyyppinen hyökkäys tehdään, todennäköisyys että se havaitaan ja todennäköisyys että hyökkäys aiheutta tietyn vaikutuksen. Riski on silloin todennäköisyyden ja vaikutuksen tulo. Riski pyritään minimoimaan poistamalla korkeimman riskin uhat, koska täysin turvalliseen tietoverkkoon ei taloudellisista syistä voi mennä. Turvallisuuden korottaminen vaikeuttaa perustoiminta ja näin aiheuttaa välillisiä kustannuksia. Välittömiä kustannuksia seuraa tietoturvamekanismien toteuttamisesta. Välillisiä kustannuksia aiheutuu hidastuneista prosesseista.

Tämä yleinen ajattelutapa, jossa verkkohyökkäyksiä yritetään kuvata riskiteorialla, on huono monestakin syystä. Ensinnäkin menetelmä käsittelee hyökkäyksen ja puolustuksen vaiheita satunnaisprosesseina, vaikka ne ovat osia hyökkääjän ja puolustajan strategiaa, näin niitä tulisi käsitellä jonkinlaisena pelinä. Tästä seuraa menetelmän toinen ongelma: millekään toiminnan vaiheelle ei pystytä asettamaan todennäköisyyksiä. Edelleen menetelmän ongelmana on hyökkäysten luokittelu: jotta jonkinlaisia todennäköisyyksiä tai vaikutuksia voitaisiin arvoida hyökkäykset tulisi jaotella hyvin yksityiskohtaisiin tyyppeihin, mutta tyyppien määrä kasvaa suureksi ja koska tyypit muuttuvat nopeasti tällaista tyyppijaottelua ei voi ylläpitää. Näin ollen, tietoverkkohyökkäyksiä ei edes pystytä mallintamaan sellaisella tavalla jolla voitaisiin käsitellä verkkotaistelua puolustusstrategioiden näkökulmasta ja laatia rationaalisia puolustusstrategioita.

5.6 Puolustautuminen verkkotaistelussa 2020

Tämä osuus käsittelee puolustautumista yleisesti tarkastelematta esitettyjä skenaarioita. Osan tarkoitus on visioida mahdollinen puolustusratkaisu tietoverkkoihin vuodelle 2020.

Verkkotaistelun puolustusmenetelmiksi tarvitaan:

1) Verkkotaistelun mallinnusmenetelmä strategioiden käsittelemiseksi
2) Uusi palvelukonsepti, johon tässä esitetään palveluverkkoarkkitehtuuria
3) Verkkohyökkäysten havaitsemismenetelmän

5.6.1 Verkkotaistelun mallinnusmenetelmän periaate

Yksi mahdollisuus parempaan mallinnukseen on käsitellä ongelmaa seuraavalla tavalla pelinä. Hyökkäys- tai puolustustoiminta on siiro. Peli sisältää tuntemattomia siirtoja eikä pelaajien strategioita voi listata tai niille asettaa saavutettavaa hyötyä. Tässä suhteessa mallinnus eroaa klassisesta peliteoriasta. Puolustaja on suojautunut tunnetuilta siirroilta. Hyökkääjä yrittää löytää uuden tuntemattoman siirron. Siirrolle ei voi asettaa vaikutusta (hyötyä), koska ei tiedetä kumpi voittaa ja millä todennäköisyydellä jos hyökkääjä tekee tämän siirron. Hyökkääjä haluaa käyttää uutta siirtoa esimerkiksi jos hän otaksuu olevansa parempi pelaaja, jos hän joutuu pakotetuksi johonkin yritykseen vaikka olisikin heikompi, tai hän vain etsii seikkailua. Puolustaja yrittää estää hyökkääjää tekemästä uusia siirtoja esimerkiksi koska hän on johdossa, eikä halua antaa tasoitusmahdollisuuksia tai jos hän on heikompi eikä uskalla antaa hyökkäysmahdollisuuksia. On alueita, joissa on enemmän mahdollisuuksia uusiin siirtoihin. Puolustajan strategiana voi olla yrittää estää

hyökkääjää pääsemästä näille alueille, esimerkiksi nostamalla välittömiä kustannuksia, esimerkiksi jo verkkohyökkäys-välineiden hankkiminen, joidenkin verkkosivujen lukeminen tai verkon skannaus voidaan tehdä rangaistavaksi vaikka kyseessä ei olekaan varsinainen hyökkäys. Rankaisu voi olla etujen poistaminen tai varsinainen rangaistus.

Puolustajan strategiana voi olla yrittää kokonaan poistaa vaaralliset alueet, esimerkiksi kehittämällä ohjelmistokehitysmenetelmiä, tietoturvapolitiikkaa tai tietoturvamekanismeja. Puolustajan strategiana voi myös olla yrittää poistaa vain ne alueet, joissa hyökkääjällä on hänen valitsemanaan aikana mahdollisuus hyökkäyk-seen. Ero näiden kahden puolustusstrategian välillä on suuri. Ensimmäisessä tapauksessa yritetään poistaa mahdollisuudet sellaiseltakin hyökkääjältä joka jaksaa odottaa mahdollisuuden ilmaantumista ja tekee hyökkäyksen heti kun tilaisuus tulee. Jälkimmäisessä strategiassa pyritään vain poistamaan sellaiset hyökkäysmenetelmät, jotka ovat aina tai riittävän usein käytettävissä. Ensimmäisen tapauksen hyökkäyksiä on esimerkiksi uuden ohjelmistovirheen hyväksikäyttö, jälkimmäisen tapauksen hyökkäyksiä ovat uuden viruksen tekeminen, palvelunestohyökkäys, takaportin asentaminen, social engineering ja sisäpuolen apuhenkilön käyttö. On luultavaa, että verkkotaistelun hyökkäysten on perustuttava jälkimmäisen tapauksen menetelmiin. Tässä mielessä verkkotaistelu eroaa perinteisistä hakkerihyökkäyksistä. Voidaan siis ehkä suojautua verkkotaistelulta Skenaarion 1 tai 4 mukaisessa tilanteessa vaikka satunnaisten hakkerien toimintaa ei voitaisikaan aina estää.

5.6.2 Palveluverkkoarkkitehtuuri

Tietoturvamekanismien käsittelystä ilmenee, ettei nykyisillä menetelmillä voida ratkaista tietoturvaongelmia. Jotta hyökkäysskenaarioilta voi sujautua tarvitaan olennaisia muutoksia infrastruktuuriin. Ensinnäkin, IP-pohjainen dataverkko on olennaisesti hajautettu prosessointiympäristö. Verkossa olevat solmut tarjoavat mahdollisuuden vaarallisten palveluiden käyttöön. Tämä on tarpeetonta, sen sijaan voidaan suunnitellla palveluverkko, joka tarjoaa vain tietyn rajoitetun määrän turvallisia palveluita.

Tietoverkon ohjelmistot tulee jakaa tietoverkkoalustaan, alustan päällä tarjottaviin palveluihin sekä tietoverkosta erotettuihin ohjelmistoihin. Nykyisellään tällaista jakoa ei selväpiirteisesti ole toteutettu, mutta tähän suuntan ollaan menemässä. Palveluiden vaatimukset ovat erilaisia kuin alustan. Palvelut tulee kehittää nopeasti ja niiden kehittämisprosessin tulee olla nopea ja kevyt. Silloin alustan tehtäväksi jää monien toiminnallisuuksien tarjoaminen palveluille. Yksi näistä toiminnallisuuksista on tietoturva.

5.6.3 Palveluiden turvallisuus

Palveluverkon tulee tarjota rajoitettu palveluluokka, kuitenkaan rajoittamatta itse palveluiden määrää koska uusia palveluita tulee voida kehittää. Tarjottujen palveluluokkien turvallisuus tulee perustua turvallisuusmalleihin ja palvelualustan turvallisuuteen. Palveluluokkien ja niiden turvallisuusmallien määrittely tämän esityksen puitteissa ei ole mahdollista, mutta käsitteen havainnollistamiseksi esitetään muutamia esimerkkejä.

Sähköposti tuntemattomien tahojen välillä
Sähköpostin tulee mahdollistaa sen, että kuka hyvänsä voi lähettää postia kenelle hyvänsä. Tämä on paperipostin peruspalvelu ja se on säilytettävä. On myös tarpeen sallia

riittävän hyvä formaatti, mikä käytännössä tarkoittaa sitä, että sähköpostin on kuljetettava tiettyjä tiedostoformaatteja. Mikäli liitetedostojen formaati voi sisältää suoritettavia ohjelmia, kuten ajettavia tiedostoja tai Word, Excel ym. makroja, niin palvelua voidaan käyttää haittakoodin lähettämiseen. Uutta tyyppiä olevien haittakoodien tunnistaminen haitalliseksi ei ole mahdollista, joten sähköpostipalvelun on estettävä tällaisten liitetiedostojen kuljettaminen. On luultavaa, että tarvitaan sähköpostipalvelun tarjoaja, hieman X.400-postin mukaisesti. On vaikea ajatella, että spontaanisti päädyttäisiin rajoitettuun sähköpostin toiminnallisuuteen ohjelmisto-toimittajien tuotteissa. Tulee myös muistaa millainen vastustus oli X.400-tyyppistä operaattorin tarjoamaa maksullista sähköpostipalvelua kohtaan. Mielipiteet eivät ole olennaisesti muuttuneet, tietoturvaa on osattava markkinoida palvelun olennaisena lisäarvon piirteenä.

Turvallinen sähköposti luotettujen tahojen välillä:
Vikka eräät valtiot pyrkivät siihen, että viranomaiset voivat aina avata salatun sähköpostin, niin ilmeisesti tarvitaan myös sähköpostipalvelu, jolla toisilleen tunnetut ja toisiinsa luotavat tahot voivat kommunikoida helpommin ja siirtää mielivaltaisia tiedostoformaatteja. Tällainen palvelu tulee suojata siten, ettei sitä voi käyttää muu kuin luotettu taho. Suojauksen on ulotuttava myös muodostetun yhteyden kaappamisen estoon, joten sähköpostin tulee olla kryptologisesti suojattu: ei välttämättä salattu mutta ainakin suojattu sähköisellä allekirjoituksella. Kryptologisia menetelmiä käyttävä posti, kuten PGP sopii muissa suhteissa tähän tarkoitukseen paitsi Web-of-trust menetelmän osalta. Web-of-trust -menetelmä ei takaa riittävää luottamusta normaalisti käytettynä. PGP ei myöskään mahdollista laillista yhteyden kuuntelua, mikä saatetaan vaatia jatkossa. IPsec saattaa joissakin käyttömenetelmissä soveltua, mutta IPsec yhteydet jouduttanee suojaamaan myös yrityksen lähiverkossa tapahtuvaa sniffausta vastaan, siis päästä päähän, jolloin laillisen yhteyden kuuntelun toteuttaminen on vaikeaa.

Web-selailu
WWW on muodostunut suosituimmaksi Internetin palveluksi ja vaikka WWW ei olekaan paras mahdollinen tekniikka hajautetun tietokannan toteuttamiseen Internetissä, niin se pysynee suosittuna. On mahdollista, että WWW korvataan jatkossa parannetulla sovelluksella: WWW:ssä on puutteellinen hakumenetelmä ja tietoa ei aina löydy hakukoneilla, esimerkiksi sama haku eri päivinä voi antaa eri tietoa. Eräs mahdollisuus on, että palveluntarjoajat kehittävät tietovälittimiä (information broker) ja loppukäyttäjät eivät haekaan tietoa suoraan Internetin hakukoneilla vaan parempien tietokantojen päälle toteutetuista tietovälittimistä. Tietoturvan osalta WWW:n ongelma on, että Web-sivullta voi ladata koneeseensa tiedostoja, joista osa voi sisältää haittakoodia. Java appletit eivät ole ongelma, koska ne toimivat javan hiekkalaatikossa, mutta tiedostojen lataaminen on ongelma. Palveluarkkitehtuurin tulisi estää tiedostojen lataaminen tuntemattomilta sivuilta. Ratkaisu voisi olla, että WWW selailu sinänsä säilytetään mutta selain muutetaan sellaiseksi, ettei se lataa tiedostoja. Silloin tulee kehittää jokin toinen tapa siirtää tiedostoja, esimerkiksi siten, että tiedosto ensin annetaan palveluntarjoajalle menetelmällä joka tunnistaa tiedoston antajan. Palveluntarjoaja yrittää tarkistaa tiedoston. Loppukäyttäjä lataa tiedoston palveluntarjoajalta. Toimintaan liittyy silloin jokin maksu. Toinen tapa on, että WWW toiminta siirtyy enenevässä määrin palveluntarjoajan tietovälittimiin, jolloin saavutetaan suurempi turvallisuus mutta Webin luonne muttuu ratkaisevasti.

VPN

Operaattorin kannalta VPN tarkoittaa yleensä MPLS VPN:ää. IPsec VPN vaatii enemmän kaistaa ja operaattorin kannalta operattorin verkko on turvallinen ympäristo eikä IPsec: in käyttö ole motivoitua. MPLS VPN vastaa lähinnä FrameRelay ja ATM tekniikalla toteutettuja puolikiinteitä yhteyksiä. Yritysten kannalta IPsec VPN saattaa olla perusteltu ratkaisu. On toisalta harkittava onko päästä päähän toteutettu salaus kuitenkin parempi ratkaisu, koska yrityksen oma verkkoympäristö ei ole turvallinen ympäristo, esimerkiksi lähiverkon osalta työntekijöiden luotettavuudelle ei ole samanlaista varmistusta kuin operaattorin verkossa tulisi olla. Käytännössä operaattoreidenkin verkossa on tapahtunut salakuuntelua, mutta tätä pyritään selkeämmin estämään ohjeistuksella kuin yrityksen verkossa. Päästä päähän salaukseen IPsec ei ole ainoa eikä välttämättä paras ratkaisu. Voidaan todeta, ettei IPsecin laaja käyttö tulevaisuudessa ole mitenkään varmaa.

Paikantamispalvelut

Loppukäyttäjän paikantaminen tietoverkon sisältämän tiedon tai verkon tai päätelaitteen tekemien mittausten avulla on teknisesti mahdollista monella tekniikalla. Uusien paikantamispalveluiden avulla toivotaan luotavan loppukäyttäjän kannalta kiinnostavia uusia palveluita. Näiden palveluiden turvallisuus perustuu palvelu-alustaan ja siihen, että on selvitettu millaisia paikantamistietoja voidaan antaa.

Loppukäyttäjän profilointi

Tietoverkko voi kerätä tilastotietoa loppukäyttäjän toiminnoista verkossa sekä säilyttää loppukäyttäjän antamia profilointitietoja. Näin tietoverkko voi kerätä mittavan tietovaraston, jonka käytöstä kiinnostuneita tahoja ovat ainakin palveluita ja tuotteita myyvät yritykset sekä näiden tietojen väärinkäyttöön pyrkivät hyökkääjät. Näiden palveluiden turvallisuus vaatii tietoturvallisen tietovaraston palvelualustassa.

Puhelupalvelu

VoIP puhelu SIP merkinannolla nähdään eräänä tärkeimpänä tulevaisuuden IP verkon palveluna. Puhepalveluun liittyy suurimpana uhkana salakuuntelu.

Puhelunohjauspalvelut

Puhelinverkon lisäarvonpalveluiden osana puhelunohjauspalvelut tarvitaan nykyisen älyverkon kaltaisten palveluiden luomiseksi. Näihin palveluihin liittyvät uhat sisältävät erilaisen kiusanteon puheluiden ohjaamisessa hätänumeroihin ja maksullisiin numeroihin suuren laskun aikaansaamiseksi. Uhkiin kuuluu myös kaaoksen aiheutaminen ja palvelunesto. Turvallisuus saavutetaan toiminnaltaan rajoitetuilla kielillä, kuten CPL, turvallisella alustalla ja hallitulla palvelukehitysprosessilla.

Älykäs kotiympäristö

Tulevaisuuden koti nähdään paljon tietoliikennettä sisältävänä rakennelmana, jossa erilaisia kotiin liittyviä laitteita voidaan ohjata tietoverkon avulla. Konseptin tietoturva vaatisi tutkimuksia.

Virtuaalikotiympäristö

Konsepti sisältää henkilökohtaisen liikkuvuuden, jossa loppukäyttäjä saa vieraassa ympäristössä samat palvelut kuin kotiympäristössään. Uhat liittyvät tietoverkon sisältämään profiilitietoon loppukäyttäjästä sekä liialliseen riippuvuuteen verkosta.

5.6.4 Palvelualustan turvallisuus

Tietoliikenneprotokollien kehityksessä käytetään yleensä protokollasuunni-ttelumenetelmiä ja niihin liittyviä työkaluja. Teletekniikassa käytettyjä ITU-T:n OSI-malliin liittyviä työkaluja ovat SDL (specification and Description Language) ja MSC (Message Sequence Chart) editorit ja validaattorit, ASN.1 (Abstract Syntax Notation no. 1) ja GDMO (Guidelines for Definition of Managed Objects) kääntäjät sekä testausta helpottava TTCN (Tree and Tabular Combined Notation)-testauskieli. Näitä työkaluja on laajennettu UML suunnittelukielellä sekä ETSI:n TTCN-3 (Test and Test Control Notation) testauskielellä ja nykyisellään testausmenetelmä soveltuu myös TCP/IP ja CORBA-pohjaisten järjestelmien kehittämiseen. UML (Unified Modeling Language) ja SDL kielet kehittyvät samaan suuntaan: UML 2 ja SDL 2000 sisältävät toistensa piirteitä ja on odotettavissa, että kehitysmenetelmät yhdistyvät jatkossa. Näillä menetelmillä pyritään mahdollisimman automaattiseen koodin generointiin, joka vähentää merkittävästi virheitä ja kehitystyökalut takaavat sangen hyvin sen, ettei näin kehitetyissä protokollissa ole puskuriylivuotoja tai eräitä muita hakkereiden käyttämiä virheitä. Työkalujen käyttö on lisääntymässä, mutta sangen hitaasti. Esimerkiksi Nokian kehitysmenetelmä on sangen automaattinen, sen sijaan monella muulla valmistajalla siirtyminen teletekniikan protokollista TCP/IP ja CORBA pohjaisiin järjestelmiin on johtanut kehitystyövälineiden käytön pienenemiseen. USA:ssa työvälineiden käyttö on ollut vähäisempää kuin Euroopassa, koska kehitykseen on perinteisesti käytetty vain heikosti tyypitettyä C-kieltä. Tämä osittain selittää miksi Unix-käyttöjärjestelmän ja TCP/IP protokollien ohjelmointivirheiden aiheuttamat tietoturvauhat ovat suurempia kuin teletekniikan puolella. Toinen ja tärkeämpi syy on, että TCP/IP avaa hakkerille mahdollisuuden päästä järjestelmään etäkäyttäjänä, toisin kuin puhelinverkko, jossa väärinkäytön mahdollisuudet ovat lähinnä salakuuntelu, palvelunesto ja laskutuksen huiputtaminen.

On todennäköistä, että työvälineiden käyttö yleistyy. Tähän joudutaan ohjelmistokehityksen vaatimuksista. Kun ohjelmistoja kehitetään kaupallisesti, ei ole aikaa siihen, että virheet paljastuvat käytössä vaan kehitysmenetelmien on oltava parempia. Samalla ne ovat myös raskaampia, mutta tämä on hyväksyttävää kaupallisessa ohjelmostokehityksessä. Se ei ole yleensä mahdollista harrastelija-maisessa ohjelmistokehityksessä, koska työvälineiden käyttöön liittyy kustannuksia, joutuu opettelemaan uusia kieliä ja hyödyt saadaan vasta jos menetelmillä tehdään paljon koodia.

Kehitysmenetelmistä puuttuu toistaiseksi työkalut ja notaatiot, joilla voidaan varmistaa kehitetyn järjestelmän tietoturvallisuus. Testaus TTCN tai TTCN-3 pohjaisesti (TTCN on ainoa standardoitu testauskieli) on musta laatikko testausta. Musta laatikko testaus ei yleensä löydä salaovia, ja myös tahattomia virheitä, kuten puskuriylivuotoja jää huomaamatta. On tarpeen kehittää uusia työkaluja. Varsinaisesti turvallisuuden tahatomien virheiden osalta varmentaa parhaiten standardien ja hyvien työvälineiden käyttö. Tahallisten virheiden, kuten salaovien ja loogisten pommien, osalta ratkaisua on etsittävä kehitysprosessin valvonnasta ja uusista tietoturvaa testaavista ja parantavista työkaluista.

5.6.5 Palveluverkkomenetelmän eroja nykyiseen Internettiin

Virusten torjuminen

Virusuhka on estettävissä mikäli sähköposti ja muut olennaiset järjestelmät (WWW) eivät siirrä kuin turvallista sisältöä. Tämä tarkoittaa sitä, että siirrettävässä tiedossa ei saa olla osia jotka johtavat ohjelmien ajamiseen käyttäjän tietämättä. Olisi täysin mahdollista kehittää turvallinen teksitin käsittelyohjelma ja rajoittaa sähköpostin siirtämien sisältötyyppien luonnetta. Tämä vaatii sen, että tiedonsiirto tapahtuu luotettavan operaattorin verkon kautta ja että Word ja Excel makrojen käyttö kielletään. On vaikea päästä tällaiseen sopimukseen lyhyellä aikavälillä, mutta vuoden 2020 skenaariossa verkon muuttuminen palveluverkoksi on mahdollista.

Avoimen koodin jakelu

Avoin ja ilmaiseksi jaettava koodi on suosittu ratkaisu Internetissä, ja sitä on myös pidetty merkittävänä vahvuutena. Tapaan sisältyy tietoturvauhkia, koska koodin hakeminen tuntemattomista palvelimista on aina uhka. Toinen ongelma on, että ilmaiseksi jaettava koodi vääristää markkinoita ja estää erityisesti pienten yritysten pääsyn markkinoille. Suuri yritys pystyy kehittämään ilmaisversiota paremman ohjelman, mutta tähän vaaditaan suuret resurssit. Vaikka ilmaiskoodia on pidetty erityisesti suurien yritysten haastajina niin käytännössä ne haittaavat pikemminkin pieniä ja uusia yrityksiä. Palveluverkkoratkaisussa koodi jaellaan erillisistä kaupallisista palvelimista eikä se ole täysin ilmaista. Palvelun tarjoaja myös varmistaa, että koodin alkuperä voidaan saada selville mikä auttaa haittakoodin eliminoimisessa.

Hajautettu prosessointi

Hajautetun prosessoinnin tarve on olemassa koska TCP sokettirajapinta ei ohjelmistokehityksen kannalta ole hyvä ratkaisu. Luotettavampaa koodia saadaan kehitettyä merkittävästi nopeammin käyttäen esitystapakerroksen tason hajautusta, esimerkiksi CORBA tai Java alustoilla. Selvä trendi middleware-alustojen laajempaan käyttöön on havaittavissa. Eräänä käytännön ongelmana palvelualustoiden laajemmassa käytössä ovat palomuurit, jotka eivät helposti salli esimerkiksi CORBA:n hajakäyttöä palomuurin yli: CORBA objektit valitsevat itse portinumeron ja ottavat yhteyden. Palomuuri yleensä estää toiseen suuntaan mielivaltaisten porttien käytön. Tämä voitaisiin ratkaista tulevaisuudessa esimerkiksi käyttämällä palomuureissa pseudosatunnaisesti hyppiviä sallittuja porttinumeroita. Kaksi pseudosatunnaisen hyppimisen tuntevaa osapuolta voi kommunikoida palomuurin läpi, mutta hakkeri joutuisi arvamaan pseudosatunnaisen porttinumerosarjan. Menetelmä voi olla melko tehokas myös palvelunestohyökkäystä vastaan, mikäli palomuurin ulkopuolella oleva verkko on suurikapasiteettinen eikä olisi tukittavissa ja palomuuri pystyisi tehokkasti hylkäämään väärät porttinumerot.

Hyökkääjien tunnistaminen ja vangitseminen vaatii ensin heidän paikallistamisensa. IP-verkko ei suoraan tällaista paikallistamista mahdollista. Mikäli hyökkääjiä ei yritetä tehokkaasti paikallistaa, puolustajan tilanne on hyvin vaikea – hyökkääjä voi kehittää uusia hyökkäysmenetelmiä ja puolustajan pitäisi osata puolustautua niitä vastaan ilman tehokkaita vastatoimia. Hajautettu prosessointialusta sisältää objektien paikallistamismenetelmän, ja tässä suhteessa olisi parempi hajautustaso.

Ohjelmistokehitys TCP/IP-maailmassa perustuu Unix ohjelmointiin, joka ei käytä kehitysmenetelmiä, joilla ohjelmistojen virheitä voidaan vähentää. Olisi toivottavaa, että ainakin palvelualustan osalta ohjelmistokehityksessä käytettäisiin kehittynempiä menetelmiä (komponenttipohjainen suunnittelu, UML & SDL, testaus ym.) Tieto-turvamenetelmien osalta tarvitaan myös täysin uusia työkaluja.

Loppupäätelmänä on, että verkon rakenne, protokollat, protokollasuunnittelu ja ohjelmistokehitys, verkon tarjoamat palvelut ym. täytyy suunnitella uudelleen. Turvallinen verkko on mahdollinen mutta nykyinen kehitys ei johda turvalliseen verkkoon. Palveluverkko joka perustuu palvelualustoihin on sangen todennäköinen kehityssuunta, mutta siihen tarvitaan hyvät turvallisuusmallit.

5.6.6 Hyökkäysten havaitsemismenetelmä

Puolustusstrategiat

Nykyinen menetelmä on puolustajan kannalta ongelmallinen: puolustaja yrittää rakentaa järjestelmänsä aukottomiksi, odottaa sangen passiivisesti (kuitenkin turvallisuutta ylläpitäen) hyökkäyksiä ja jos hyökkäys tehdään ja havaitaan, yrittää saada hyökkääjän edesvastuuseen teoistaan. Muita strategioita ovat esim. vastahyökkäys. Vastahyökkäyksen tekeminen saattaa johtaa ongelmiin ja toisena ongelmana on hyökkääjien paikallistaminen. Hyökkääjien tunnistaminen ennalta on yksi mahdollisuus. Edelleen voidaan harkita hyökkäyksen seuraamisvaikutusten, lähinnä rangaistusten, koventamista, mutta ne ovat jo sangen kovat.

Hyökkäysten havaitseminen

Saattaa olla tarpeen rakentaa tietojärjestelmä, jolla tietoverkkoihin kohdistuvat hyökkäykset saadaan selville, siis suuri hajautettu IDS järjestelmä. Nykyään IDS järjestelmiä on monissa yrityksissä, mutta yhdistävänä tekijänä on vain CERT, joka on tietoa keräävä ja neuvoa antava elin, ei tietojärjestelmä.

Tämä johtaa kysymykseen millä tasolla puolustusmenetelmä on: tuleeko puolustusvoimien suojata maan rajoja myös tietoverkoissa, vai onko puolustus kunkin yrityksen oman verkon rajalla. Mikäli maata yritetään puolustaa fyysisessä mielessä verkkohyökkäyksiltä, tarvitaan verkotettu IDS järjestelmä. Sellainen saatta olla mahdoton sen keräämän tietomäärän vuoksi, mutta toisaalta Suomen tietoverkkoyhteydet ulkomaille ovat sangen harvojen pisteiden kautta.

Internetin sisällon seuraaminen

Internetin käyttö vaarallisen tai laittoman tiedon julkiseen levittämiseen pyritään estämään. Pääsy tiettyihin www-osoitteisiin voidaan estää yritysten tai ISP (Internet Service Provider) palvelun tarjoajien palomuureilla. Sisällön tarkistaminen on osin jo mahdollista automaattisesti ja XHTML:n (XML-pohjainen HyperText Markup Language) otsaketietojen tarkistamisella tätä suodatusta voidaan edelleen parantaa. Näillä menetelmillä ei voi estää henkilöä, joka haluaa päästä tietyille sivuille pääsemästä sinne jonkin toisen yhteyden kautta, mutta näin hidastetaan tietojen leviämistä laajemmin niille, jotka eivät niitä erityisesti etsi. Laittoman sisällön osalta viranomaisten tulee seurata Webin sisältöä sopivien hakusääntöjen avulla. Toistaiseksi esimerkiksi hakkerointisivut ovat täysin

laillisia ja helposti löydettävissä, edelleen ohjeita hakkerointiin ja valmiita skripteja löytyy tietoturvayritysten sivuilta, joissa niitä pidetään tietoturvaa edistävinä sivuina.

Ei-julkiseksi tarkoitetun sisällön seuranta, esimerkiksi sähköpostien lukeminen ja salakuuntelu, on ollut esillä menetelmänä estää terroristien ja rikollisten yhteydenpitoa ja tunnistaa mahdolliset väärinkäytökset ennakolta. Tämän luonteinen toiminta on laitonta ja viranomaisetkin tarvitsevat siihen valtuudet. Valtuuksien laajentamisella voi olla arveluttavia seurauksia ja eräänä täysin mahdollisena tulevaisuusskenaariona voidaan pitää Orwellimaista 1984 skenaariota, jossa tietoverkon sisältämä erittäin suuri tietomäärä on viranomaisvalvonnassa.

5.7 Puolustautuminen verkkotaistelun eri skenaarioissa

Tässä osassa käsitellään eri skenaarioiden erityispiirteitä tukeutuen osuuksiin 5.5 ja 5.6.

5.7.1 Puolustautuminen skenaariossa 1

Skenaario 1 kohdistuu yhteiskuntaan ja 4.5 mukaisesti hyökkääjä voi nykyisessä verkossa aiheuttaa kaaosta ja tuhoa käyttämällä uusia ohjelmistovirheitä hakkerointiin, uusia viruksia, jotka läpäisevät aluksi virustarkistuksen, arvaamalla heikkoja salasanoja ja hyödyntämällä huonoa turvallisuuspolitiikkaa, sekä hidastaa toimintoja palvelunestohyökkäyksillä. Skenaariossa 1 hyökkääjän päämäärä on paljolti mielipiteen muokkaus. Käytettävissä olevilla menetelmillä saatanee aikaan toivottu vaikutus, toisaalta puolustaja voi Skenaariossa 1 paljolti hallita kansalaisten mielipiteen muodostusta tiedotusvälineiden kautta. Hyökkäysten kohdistaminen energianhuoltoon, esimerkiksi sähkön jakelun häiritseminen, saisi aikaan käytännön vaikeuksia, muttei luultavasti suurempaa vaikutusta. Perl Harbor II skenaariossa on kuvailtu suuri joukko eri menetelmiä, millä Skenaarion 1 hyökkäystä voisi tehostaa. (Perl Harbor II on yleisesti tunnettu informaatiosodankäyntiskenaario, jossa joukko toisilleen aiemmin tuntemattomia henkilöitä tutustuu Internetin keskustelusivuilla ja jostain syystä päättää saattaa maailman kaaokseen Internetin kautta tehtävällä verkkohyökkäyksellä. Skenaariota ei pidetä uskottavana, sen tarkoitus on lähinnä osoittaa, ettei tunnettujen terroristiryhmien muodostama uhka ole ainoa verkkotaistelu-uhka. Skenaariossa kuvaillut lukuisat hyökkäysmenetelmät ovat kuitenkin periaatteessa toimivia.)

Mahdollinen uhka, erityisesti puolustusvoiminen järjestelmissä, on, että Suomeen hankittu ulkomailla kehitetty teknologia olisi vanhentunutta tietoturvan osalta, jolloin kolmannen osapuolen tiedustelu olisi tietoinen ongelmista ja voisi käyttää niitä verkkotaistelussa. Suomalainen osapuoli ei kuitenkaan olisi tietoinen näistä jo korjatuista ongelmista. Tämä uhka kohdistunee enemmänkin ase- ja sensori-järjestelmiin. Esimerkiksi tutka ei ehkä näytä kaikkia kohteita.

On kuitenkin luultavaa, että nykyinen hyökkäys Skenaarion 1 tilanteessa olisi pikemminkin perinteinen terroristi-isku kuin verkkohyökkäys. Terroristi-iskun vaikutus maassamme olisi samankaltainen kuin maissa, joissa tällaisia tapahtuu.

Kohdassa 5.6 esitetty ratkaisuehdotus voisi olla osa Skenaarion 1 puolustus-menetelmää vuonna 2020. Todennäköisesti hyökkäys Skenaarion 1 tilanteessa olisi myös vuonna 2020 pikemminkin perinteinen terroristihyökkäys. Verkkotaistelun uhka olisi saatu pienennettyä paremmalla turvallisuusarkkitehtuurilla.

5.7.2 Puolustautuminen skenaariossa 2

Skenaariossa 2 Suomi on sodassa valtion kanssa, joka on teknologisesti korkealla tasolla ja pyrkii informaatioylivoimaan. Strategisen iskun osana on verkkosodan-käyntiä. Päämääränä on lamaannuttaa yhteiskunnan elintärkeät toiminnat ja puolustusvoimien johtamisjärjestelmä. Skenaario 2 voisi syntyä esimerkiksi seuraa-vissa tilanteissa vuonna 2020: Suomi joutuu yksinään sotaan Venäjän kanssa, EU ajautuu sisällissotaan, EU kehittyy Euroopan Yhdysvalloiksi, NATO lopetetaan ja Euroolan Yhdysvallat ajautuu sotaan USA:n kanssa, NATO ajautuu sotaan Venäjän kanssa sekä Suomi yrittää irroittautua Euroopan Yhdysvalloiksi kehittyneestä EU:sta. Mikään näistä skenaarioista ei ole todennäköinen nykyisten näkymien pohjalta, mutta Skenaarion 2 käsittelemiseksi tällaiset tilanteet on oletettava mahdollisiksi. 18 vuotta ei ole niin pitkä aika, että hyökkääjän strategia olennaisesti eroaisi USA:n nykyisestä strategiasta. Sota alkaisi voimakkaalla ilmaiskulla, jossa täsmäpommituksin vaikutettaisiin asejärjestelmiin ja tämän esityksen kannalta kiinnostaviin tieto- ja tietoliikennejärjsetelmiin. Verkkosodan-käynti olisi osana ensi vaiheen toimintaa ja sen päämääränä olisi lamaannuttaa puolustusjärjestelmät ja puolustustahto.

Hyökkääjän käytettävissä olisi esimerkiksi seuraavia menetelmiä: COTS pommit, Suomeen myytyjen COTS-ja MIL-tuotteiden suurempi tuntemus, virukset sekä salakuuntelu.

Puolustusvoimien verkon turvallisuus perustuu linkkitasolla salattuihin yhteyksiin ja verkon solmujen suojaamiseen fyysiseltä ja elektroniselta vaikuttamiselta. Fyysinen suojaus on tämän esityksen ulkopuolella, ja otetetaan, että se on riittävä. Jokainen salaus voidaan periaatteessa purkaa, mutta voidaan olettaa, että jos salaisilla salausmenetelmillä salattu data salataan tunnettuilla vahvoilla salausmenetelmillä kuten AES ja RSA, saadaan salaus, jonka purkaminen on käytännössä mahdotonta. Epätodennäköisenä, mutta mahdollisena uhkana tulee muistaa rinnnakkais-menetelmien kehittyminen, esimerkiksi riittävän monta rinnakkaista toimintaa tekevän kvanttitietokoneen oletetaan olevan käytettävissä 2050, mutta saattaa olla, että sellainen olisi olemassa jo 2020. Kehittynyt kvanttitietokone vanhentaa nykyiset salausmenetelmät. Toisaalta kvantti-informaatioteknologia myös mahdollistaa salauksen, jota ei koskaan voi purkaa.

Oletetaan (melkoisella varmuudella), ettei tällaisia koneita eikä muutakaan suuressa mitassa rinnakkaista salauksen purkajaa ole olemassa vielä 2020. Silloin kuljetus-, verkko-, tai linkkitason salaus antaa sangen suuren varmuuden sille, että päästäkseen verkkoon hyökkääjän tulee saada käyttöönsä verkossa oleva laite. Tämä voi tapahtua esimerkiksi varastamalla tunnisteet, valloittamalla laite ja käyttämällä sisäpuolella jo olevia vakoojia. Satunnaiseen haittakoodin levittämiseen perustuva menetelmä tuskin antaa hyökkääjälle riittävää varmuutta, joten virusten leviäminen vahingossa levykkeiden avulla operatiiviseen verkkoon ei todennäköisesti ole menetelmä, jota hyökkääjä kayttää.

Verkon sisäpuolelle päässyt henkilö voi muuttaa itsensä pääkäyttäjäksi koodin virheiden avulla, koska puolustusvoimien tietokoneet eivät ole korkeaa tietoturva-tasoa. Tämän jälkeen hän voi tehdä kyseisessä koneessa mitä vain. Hän voi jatkaa muihin koneisiin, esimerkiksi hakkeroimalla tai lähettämällä viruksen, jossa on takaovi. Tällaiseltä toiminnalta voi suojautua siten, että verkossa on koneissa Host-IDS, joka tekee lokitietoa toiselle koneelle, johon hakkeri ei pääse. On myös hyvä asentaa verkkoon N-IDS. Se ei tunnista mitään salattua tietoa, joten järjestelmä tuntuu aivan turhalta koska kaiken tiedon pitäisi olla salattua. Kuitenkin, hakkerin yritykset päästä verkon toisiin koneisiin ovat usein salaamattomia, joten N-IDS tunnistaa ne. On tarpeen saada johonkin toiseen ja luotettuun koneeseen lokitietoa kaikista yrityksistä asentaa uusia ohjelmia koneisiin. Näin hakkerin toiminta voidaan havaita ennen kuin hän saa koneen haltuunsa.

COTS-tuotteissa oleva looginen pommi on usein mainittu ja täysin mahdollinen uhkakuva, jossa COTS-tuotteeseen on tietoisesti asennettu koodi, joka laukeaa jollain liipaisulogiikalla. Pommin voi laukaista liipaisulla, joka tarvitsee viestin, mutta tämä on hyökkääjän kanalta epävarmaa sillä viestin välitys on voitu estää. On luultavinta, että liipaisu on aikasidonnainen. Tällaiselta loogiselta pommilta voidaan suojautua esimerkiksi siten, että toiminnat peilataan varakoneelle, jonka kello on jäljessä. Voi myös peilata toimintoja konelle, jonka kello on edessä ja yrittää saada loogisen pommin käyntiin etuajassa, mutta tämä onnistuu vain jos varakoneessa on looginen pommi ja se laukeaa. Erityyppisten laitteiden käyttöä on usein ehdotettu tahattomien ja tahallisten virheiden vaikutuksen pienentämiseksi, mutta se pienentää järjestelmän hallittavuutta ja aiheuttaa yhteentoimivuusongelmia.

Toinen uhka COTS-tuotteissa ja ulkomaisissa sotilastuotteissa on, että järjestelmän kehittäjät tuntevat koodin paremmin. Usein koodissa on tunnettuja heikkouksia, tai ainakin tiedetään milla pienillä muutoksilla koodiin saa luotua takaportteja. Tämä heikkous olisi hyvä perustelu kehittää eurooppalaista koodia kansainvälisten standardejen pohjalta, TCP/IP on olennaisesti amerikkalainen protokollaperhe. Vaikka Suomessa on korkeaa osaamista tietoliikennealueella, ohjelmistopuolella kehitys on pääosin ulkomaista. Erityisesti korkean turvallisuustason järjestelmiin hakkerointi vaatinee sisäpiirin tietoa koodista, joka on lähinnä vain ohjelmisto-kehittäjillä.

5.7.3 Puolustautuminen skenaariossa 3

Skenaariossa 3 jokin ulkomainen yritys yrittää estää teknologista kehitystä Suomessa. Verkkosodankäynnillä pyritään vakoilemaan yrityssalaisuuksia, estämään asiakkaan ja yrityksen toimintaa palvelunestohyökkäyksin ja tuhomamaan yrityksen osaamista esimerkiksi viruksilla. Hitaasti dataa korruptoivat virukset soveltuvat parhaiten tällaiseen toimintaan. Verkkosodankäynti on pitkäaikaista ja päämääränä ovat taloudelliset menetykset ja markkinaosuuden pieneneminen hyökkäyksen kohteena olevalle yritykselle.

Verkkosodankäynti yrityksiä vastaan on samassa mielessä yleisiä pelisääntöjä vastaan kuin vastaava fyysisiin aseisiin perustuva toiminta olisi. Tästä johtuen tätä verkkosodankäyntimuotoa voidaan parhaiten vastustaa laeilla ja säädöksillä ja toiminnan estäminen on poliisin tehtäviä. Yrityksen tulee tehdä toiminta riittävän vaikeaksi käyttämällä hyviä tietoturvamekanismeja. Nykyisellään tietoturvame-kanismit eivät estä hakkerointia ohjelmistovirheitä käyttäen, virusten ja muun haittakoodin lähettämistä, eivätkä poista

kokonaan palvelunestohyökkäyksiä. Palveluverkkokonsepti toteutuessaan voisi poistaa nämä uhat pääosin vuonna 2020. Skenaarion 3 verkkosodankäynnin muoto ei mielestäni ole sellainen uhka, että puolustusvoimien tulisi siihen erityisesti varautua. Kysymys eri maiden lakien ja kansainvälisen lainsäädännön kehittämisestä on polittinen. Tällä verkkosodan-käyntimuodolla voi olla strategisia tavoitteita, kuten USA:n vientirajoituksilla itäblokin maihin, ja nämä tavoitteet voivat johtaa todellisiin strategisiin vaikutuksiin, mutta kysymys on perimmiltään poliittisesta toiminnasta.

Skenaario 3:a suurempi uhka on, että teknologiakehitys suosisi jonkun maan hyvin hallistsemaa teknologiaa, jolloin siitä seuraisi merkittäviä etuja teknologiaa hallitsevan maan teollisuudelle. Täysin laillisilla toimilla saadaan siis sama vaikutus kuin Skenaario 3 verkkosodankäynnillä. Jos verkkosodankäyntiä riittävästi vaikeute-taan, Skenaarion 3 tilanteessa hyökkääjä siirtyy tällaisten laillisten keinojen käyttöön. Kansainvälisellä standardoinnilla pyritään estämään tällaista kehitystä strategisesti tärkeillä aloilla, mutta defacto standardit edistävät tällaista kehitystä. Voitanee todeta, että TCP/IP teknologia on paljolti amerikkalaista tekniikkaa, ja jossain määrin huonommin edustettua eurooppalaisissa yrityksissä. Tilanne on päinvastainen esimerkiksi GSM:n osalta.

Skenaario 4.

Tässä skenaariossa Suomi tekee verkkotaistelun menetelmin vastahyökkäyksen, mahdollisesti jo ennen odotettavissa olevan Skenaarion 2 hyökkäyksen alkamista. Koska hyökkääjän pitää olla paikanettavissa, skenaario ei sovellu Skenaarion 1 vastatoimeksi. Sen käyttö Skenaariossa 3 olisi arveluttavaa. Sen sijaan Skenaarion 2 vastatoiminen osana tällainen hyökkäys olisi luonteva. Kysymys on, mitä tällainen hyökkäys voisi saavuttaa? Vaikka Suomessa onkin korkeaa tietoliikenneosaamista, niin ei ole luultavaa, että löydettäisiin muiden maiden kriittisiä järjestelmiä kehittäneitä henkilöitä, joten sisäpiirin tieto heikkouksista olisi vähäistä. Olisi keskityttävä hyökkäyksiin, jotka eivät tarvitse tällaista tietoa. Palomuurikohdan lopussa on kuvailtu yksi menetelmä, joka on periaatteessa mahdollinen useimpiin verkotettuihin kohteisiin eikö vaadi erityistä tietoa järjestelmästä. Se perustuu osittain huonoon tietoturvapolitiikkaan, siis käyttäjien hyväuskoisuuteen ja välinpitämä-ttömyyteen. Nämä ominaisuudet ovat toisaalta hyvin yleisiä.

Skenaariossa 4 ei voida valita hyökkäysajankohtaa yhtä hyvin kuin Skenaariossa 1. Tästä seuraa, että virusten käyttö ei ole yhtä helppoa. Ne yleensä hyödyntävät joitakin uusia heikkouksia ja ohjelmistovirheitä. On mahdollista löytää joukko toimivia hyökkäysmenetelmiä korkean turvallisuustason kohteisiin, lähinnä palomuurikohdan menetelmän kaltaisia osin "social engineerin"–tyyppisiä tapoja. Myös DDoS hyökkäykset yleensä ovat mahdollisia. Yleensä yhteiskuntaan kohdistuvia hyökkäy-ksiä on helpompi luoda. Niillä ei ole olennaista vaikutusta yhteiskunnan toimivuuteen, mutta jonkinlainen psykologinen vaikutus niillä voi olla. On sangen paljon kohteita, jotka eivät seuraa riittävän nopeasti tietoturvapäivityksiä. Niihin hakkerointi onnistuu silloin tunnetuilla aukoilla. Näillä menetelmillä voidaan luoda kaaosta, muttei juuri muuta vaikutusta.

Mikäli Skenaariota 4 pidetään tarpeellisena, olisi perustettava hakkerijoukot koska suomalaisten tietoliikenneammattilaisten osaaminen on pikemminkin tietoturvallisten järjestelmien rakentamisessa kuin hakkeroinnissa. Hakkerointi-tietämys on luonteeltaan nopeasti vanhenevaa ja ammatillisessa osaamisessa tarpeetonta detaljitietoa, kuten muiden koneiden salasanojen etsimistä ja varastointia ym. Tiettynä indikaationa siitä,

että suomalaisia korkean tason hakkereita ei ole paljon on se, ettei heitä ole jäänyt kiinni kuin muutama. Tähän voi vaikutaa yleinen mielipide, jota kuvastaa se, että suomalaisessa yhteiskunnassa omaisuusrikollisuuden määrä on sen verran pieni, että suojautuminen esimerkiksi varkauksien varalta on huomattavasti vähäisempää kuin monessa Keski-Euroopan maassa. Tämä mielipide riittävästä turvallisuudesta näkyy myös tietoturvaasioissa ja hakkeritoiminnan vähäisyytenä. Toisaalta perustaso esimerkiksi suomalaisilla tietotekniikan ja tietoliikenteen opiskelijoilla on korkea. Verkkotaistelun käyttö Skenaarion 4 tilanteessa on ollut vähäistä, mutta esimerkkinä mainitaan jugoslavialaisten hakkereiden yritykset USA:ta vastaan Jugoslavian sodan aikana. Vaikutukset jäivät vähäiseksi. Tästä huolimatta tätä sodankäynnin tapaa tulisi tarkastella Skenaarion 2 yhteydessä ja tarkemmin selvittää sen mahdollisuuksia. Kyseessä on kuitenkin yksi harvoista tavoista vastata Skenaarion 2 hyökkäykseen.

5.8 Yhteenveto verkkotaistelun puolustusmenetelmistä

Skenaarioiden 1 ja 3 mukaisia hyökkäyksiä yritetään torjua kohdassa 5.3 esitetyillä menetelmillä, mutta näitä puolustusmentelmiä vastaan voidaan käyttää useita toimivia hyökkäyksiä. Mikäli Skenaarion 1 hyökkäyksiä pyritään kokonaan torjumaan tarvitaan parempia tietoturvamalleja. Kohdassa 5.6 on luonnosteltu eräs ratkaisu. Skenaario 3:n hyökkäyksien osalta poliisin toiminta verkkohyökkäysten estämiseksi on avainasemassa, mutta 5.6 ratkaisu on tässäkin avuksi. Skenaario 2 on puolustus-voimien kannalta tärkein uhkakuva, ja sen vastatoimena tehtävä Skenaarion 4 mukaisen verkkohyökkäyksen teho tulisi selvittää. Mikäli Skenaario 4:ää halutaan käyttää, tarvitaan enemmän hakkerointitietoa ja koulutusta.

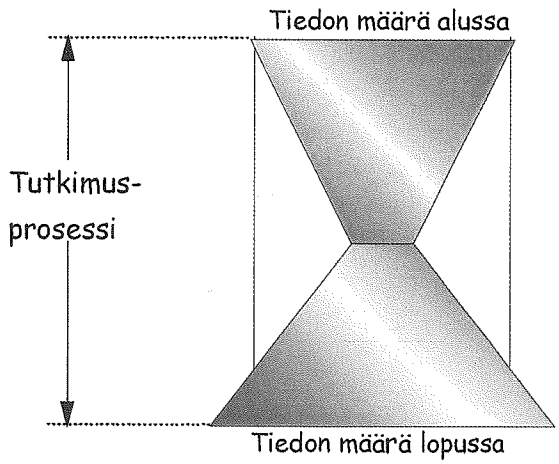
6. DISKUSSIO – MITÄ VERKKOTAISTELU 2020 – HANKKEEN JÄLKEEN ?

Mika Piiroinen
majuri, viestitaktiikan opettaja
Maanpuolustuskorkeakoulu, Taktiikan laitos

Tässä artikkelissa tehdään yhteenveto tämän julkaisun muista artikkeleista sekä pohditaan, mitä tuloksia verkkotaistelu 2020-hankkesta saatiin ja miten tutkimusta voitaisiin jatkaa.

6.1 Saavutettiinko tutkimuksen tavoite ?

Komentaja, kauppatieteiden tohtori Ilkka Haapalinna määritteli tutkimuksen merkityksen vuonna 1997: *" Tutkimus on onnistunut, mikäli tutkimuksen lopussa saavutetun tiedon määrä on isompi kuin tutkimuksen alussa käytössä ollut tieto."* Määritelmäänsä komentaja Haapalinna tarkensi seuraavalla kuvalla.



Lähde: Komentaja Ilkka Haapalinna; Tutkimuksen onnistumisesta (luento YEK 45/kesä 1997)

Verkkotaistelu 2020-hankketta voidaan pitää onnistuneena, jos mittarina käytetään Haapalinnan esittämää määritelmää. Toisaalta tähän työhön osallistuneet ovat ensimmäisenä myöntämässä, että Verkkotaistelu 2020 ei ole kattava tutkimus asiasta.

6.2 Työssä on paljon puutteita...

Nyt kun julkaisu on valmis, on kysyttävä, mitä voitaisiin tehdä toisin. Puolustusvoimissa tukeudutaan informaatiosodankäynnin määrittelyissä ennen kaikkea amerikkalaisiin näkemyksiin. Tämä tulee hyvin esille, kun verrataan ev evp Alan Campénin jakoa informaatiosodankäynnissä [Information Warfare Definitions, Signal July, 1995, s. 68] ja Puolustusvoimissa käytössä olevia määritelmiä [PE johtjärj-os:n muistio 31.3.2003]. Erot määritelmissä ovat vähäisiä. Syynä määritelmien samankaltaisuuteen on tarve yhdenmukaistaa myös käsitteet.

Tämä tukeutuminen amerikkalaisiin käsityksiin näkyy myös tässä hankkeessa. Sakari Ahvenaisen artikkeli pohjautuu pitkälti yhdysvaltalaisiin käsityksiin. Tutkimuksellisesti olisi ollut mielenkiintoista saada mukaan artikkeli, jossa olisi esitetty venäläisten käsityksiä verkkosodankäynnistä. Ja ennen kaikkea venäläisten itsensä kirjoittamana. Nyt valinta tehtiin toisin. Valintaan osaltaa vaikutti se, että Taktiikan laitos on julkaissut vuonna 1999 Jorma Saarelaisen tutkimuksen venäläisestä informaatiosodankäynnista [Taktiikan laitoksen julkaisuja, julkaisusarja 1, 1/1999] sekä vuonna 2001 käännöksen Venäjän Federaation informaatioturvallisuuden doktriinistä [Taktiikan laitoksen julkaisuja, julkaisusarja 3, 1/2001].

Tutkimuksen aikana havaittiin, että hyökkäys-puolustus- skenaarioidea osoittautui haastavaksi. Skenaarioiden muodostaminen kävi vielä kohtuullisen helposti. Työn edetessä havaitsimme, että menetelmällisesti, sotilaallisesti ilmaisten taktis-teknisellä tasolla, verkkohyökkäykset ovat lähellä toisiaan. Skenaariot olisi pitänyt muodostaa niin, että niihin olisi luotu myös erilaiset ja yksityiskohtaisemmat rakenteet tietoverkoille ja –järjestelmille.

Jouduimme luopumaan tavoitteestamme, jossa olisimme käsitelleet skenaariot järjestyksessä ja skenaario kerralla kirjoittaneet ensin hyökkäyksen toteuttamisen ja tämän jälkeen puolustusratkaisun kyseiseen hyökkäykseen. Tämän jälkeen olisi työn alle otettu seuraava skenaario. Kyseisen ratkaisun toteuttaminen olisi vaatinut huomattavasti enemmän yhteistä aikaa kuin mitä meillä nyt oli käytössä. Mikäli olisimme toimineet esitetyllä tavalla olisimme todennäköisesti saaneet aikaan tarkemmat ja enemmän yksityiskohtiin pureutuvat kuvaukset, miten verkkohyökkäys ja –puolustus pitäisi toteuttaa. Täten olisimme pystyneet konkrettisoimaan asioita vielä enemmän.

Toisaalta on muistettava, että jokaisen skenaarion tarkka määrittely ja käsittely myös sitoo tutkimusta voimakkaasti. Samalla rajataan käsittelyn ulkopuolelle monia muita mahdollisia skenaarioita. Tämän hankkeen eräs oppi on myös se, että tulevaisuuden skenaarioita laadittaessa innovatiivisyys ja mielikuvitus on vapautettava kaikista kahleista. Se, että nyt verkkohyökkäykset osoittautuivat menetelmällisesti samankaltaisiksi, osoittaa sen, että tutkimukseen osallistuneiden mielikuvitus ei sittenkään riittänyt.

6.3 Artikkeleista

Sakari Ahvenaisen artikkeli verkkosodan historiasta ja käsitteen kehittymisestä antaa hyvän perustan asiasta kiinnostuneelle. Lukija varmasti välillä pohtii, voiko verkkosodan kehittymistä jakaa niin moneen vaiheeseen kuin Ahvenainen esittää. Kysymyksessä on

vain kymmenen vuotta vanha asia. Määrätyn selityksen asiaan antaa, kun muistetaan, että Internet-maailmassa, mihin verkkosotakin liittyy, yksi "vuosi" on kolme kuukautta pitkä ja kalenterivuosi sisältää itseasiassa kolme - neljä internet-vuotta.

Sotilaspedagogit pohtivat tällä hetkellä muun muassa cypersotaa ja miten siitä tulevat vaatimukset huomioidaan koulutuksessa. Tähän työhön saadaan uudenlainen perusta, kun pohjaksi otetaan Ahvenaisen esittämä jako erityyppisistä kybersodista.

Ahvenainen kirjoittaa Netwar Centric Warfaresta, verkostosodankäynnistä, jonka mukaisesti Yhdysvaltojen puolustusministeriö on esittänyt USA:n asevoimien uudellenorganisointia. Mielenkiintoiseksi verkostokeskeisen sodankäynnin tekee se, että kyseinen toimintatapaa on valittu myös Ruotsin puolustusvoimien strategiseksi toimintatavaksi (Nätverksbaserat försvar - NBF).

Mitä verkostokeskinen sodankäynti tai puolustus sitten on ? Kuten Ahvenainen esittä yksiselitteisen määritelmän antaminen on vaikeaa, koska kysymyksessä on monista eri tasoista ja niiden välisestä vuorovaikutuksesta koostuva kokonaisuus. Verkostokeskeisen sodankäynnin ajatus on mielenkiintoinen. Tästä syystä asian tutkimiseen tulisi panostaa resursseja. Tutkimuksessa tulisi selvittää muun muassa verkostokeskeisen sodankäynnin riskit sekä mitä muutoksia verkostokeskeinen sodankäynti aiheuttaa operaatiotaidon ja taktiikan tai johtamisen opetukseen. Tätä kirjoittaessa on Persianlahden toinen sota alkuvaiheessa. Tällä hetkellä on näyttänyt siltä, että sotaa on käyty hyvin perinteisellä tavalla. Tutkimuksen kannalta onkin haaste selvittää, miten verkostokeskeisen sodankäynnin-oppi on toteutunut tässä sodassa.

Ahvenainen on pysytellyt hänelle annetussa tehtävässä selvittää verkkosodan historiaa ja käsitettä. Johtopäätösten tekeminen on jätetty lukijalle. Työn lopputuloksena esitetty verkkosodan uusi viitekehys on mielenkiintoinen. Tästä viitekehyksestä voidaan nostaa esille kolme laajaa kokonaisuutta, jotka Ahvenaisen mukaan painottuvat tulevaisuudessa. Nämä kokonaisuudet ovat 1) tekniikan ja sen tuominen mahdollisuuksien ja rajoitusten ymmärtäminen, 2) ymmärtää, miten ihmisten mieliin vaikutetaan sekä 3) verkostoituminen ja sen tarjoamat mahdollisuudet.

Helokunnas, Laukkanen ja Viitanen nostavat artikkelissaan esille tiedon merkityksen korostumisen. Kuten artikkelissa esitetään tieto ja osaaminen ovat nousseet perinteisen tuotantotekijöiden rinnalle. Mikäli joku asia hallitaan hyvin, voidaan sitä pitää organisaatioon kannalta merkittävänä pääomana, jolle on määritettävissä selkeä taloudellinenkin arvo. Tätä ajattelua tukee se, että pörssimaailmassa eri pankkiiriliikkeiden analyytikot arvioivat yrityksistä yhä enemmän niiden osaamista ja ennen kaikkea yrityksien johdon kyvykkyyttä ja uskottavuutta. On olemassa selkeätä näyttöä siitä, että kahden samalla alalla ja samassa tilassa olevien yritysten pörssikurssien välillä oleva ero voidaan selittää vain yrityksen johdon roolilla.

Tiedon merkitys –artikkeli nostaa esille kysymyksen eri tietojärjestelmien tuottamasta tiedosta ja sen luonteesta. Tähän perustuen voidaan kysyä, ymmärtääkö eri tietojärjestelmien käyttäjät, että tietojärjestelmään tuottama tieto on dataa tai korkeintaan osittain informaation tasoista tietoa. Tietämys ja osaaminen on ihmisten tehtävä ja kompetenssialue. Meidän on ymmärrettävä, että esimerkiksi JOTI-tietojärjestelmä ei tee päätöksiä, niin kuin välillä virheellisesti esitetään. Kyseinen tietojärjestelmä tuottaa tilannekuvan.

Käyttäjien on myös muistettava pohtia kyseisen tilannekuvan oikeellisuutta.

Tiedon hyödyntämistä nousee haaste myös koulutukselle. Osaavatko tietojärjestelmien käyttäjät lukea oikein tietojärjestelmien luomaa kuvaa siten, että tietämyksen prosesseille eli perustelulle, päättelylle ja ennen kaikkea sotilasjohtajan tärkeälle ominaisuudelle epävarmuuksien hallinnalle on riittävä perusta. Olemmeko me tulossa toiminnassa siihen tilanteeseen, jossa tilannekuvaa ei voida muodostaa kuin koneiden avulla. Jos näin on, niin nouseeko johtajan yksi tärkeimmäksi ominaisuudeksi oppia ymmärtämään konetta ja tätä kautta luoda siitä haluamansa tilannekuva, joka palvelee päätöstä.

Millaisia johtajia meidän on koulutettava, että he kykenevät muodostamaan tilannekuvasta (data ja informaatio) oikeanlaisen tilannekäsityksen (tietämys). Onko meidän otettava yhdeksi opetuksen päätavoitteeksi se, miten oppijat saadaan muodostamaan käytössä olevasta tilannekuvasta mahdollisimman oikea tilannekäsitys ?

Näyttäisi siltä, että tulevaisuudessa yhä suurempi haaste on oppia tunnistamaan ja erittelemään tärkeä informaatio ja tärkeä tieto (ihmisissä). Toisaalta tähän liittyy myös suuri paradoksi, toisille ihmisille hyvinkin vähäarvoinen tieto voi olla toiselle kriittisen tärkeä. Tämän jälkeen olisi keskityttävä ennen kaikkea tärkeän tiedon suojaamiseen siten, että sen eheys, käytettävyys ja luottamuksellisuus säilyy mahdollisimman hyvänä.

Mikko Hyppönen esittää artikkelissa mielenkiintoisia näkemyksiä tulevaisuudesta, kuten englannin kielen roolista ja osuudesta sekä muistisiruista ja niiden kapasiteetistä. Skenaarioita ja niissä esitettyjä yksityiskohtia on samalla kertaa pelottava ja hauska lukea. Näitä asioita olisi mielellään lukenut pidempäänkin. Todellisuus todennäköisesti onnistuu hämmästyttämään meidät kaikki.

Toivottavasti eri skenaariot saavat lukijan pohtimaan, mitä kaikkea verkkohyökkäyksillä voidaan saada aikaan. Pelottavaa on se, että asiat, jotka me kuvittelemme tapahtuman tulevaisuudessa, kyetäänkin toteuttamaan jo tänään. Mitä sitten kyetään tekemään tulevaisuudessa ? Kuten Hyppönenkin toteaa uhkakuvat muuttuvat vuosi vuodelta pahemmiksi. Yksi suurimpia haasteita on, miten kyseiset uhkakuvat saadaan ihmisten tietoisuuteen. Esimerkiksi MpKK:ssa ei opiskelijoille ole toistaiseksi opetettu verkkosodan mahdollisuuksia ja keinoja. Tähän yksi syy saattaa olla se, että me pidämme teoriaa ja käytäntöä eri asioina. Onko niin, että me emme satsaa asiaan resursseja, koska me emme ole vielä nähneet todellista lamauttavaa verkkohyökkäystä.

Hyppösen artikkelin merkittävin johtopäätös on, että käytettävät tietokoneet pitäisi eristää julkisista verkoista, jos halutaan todellista korkean tason tietoturvaa. Puolustusvoimat on toistaiseksi pyrkinyt toimimaan Hyppösen esittämällä tavalla. Tosin ratkaisut on toteutettu siten, että on suojattu kaikki järjestelmät ilman, että olisi eriteltu mikä on kriittistä ja vähemmän kriittistä tietoa. Eri kysymys onkin, onko miten tähän tilanteeseen on ajauduttu ? Onko niin, että tärkeätä tietoa ei ole aikanaan osattu tai haluttu erotella kuin salattavuussyistä.

Jormakan artikkelissa lähestytään verkkopuolustusta teknisestä näkökulmasta. Artikkeli sisältää myös ennustuksia tulevaisuuden johtamisjärjestelmien teknillisistä ratkaisuista. Täten kyseinen artikkeli palvelee laajemmalti koko Taistelukenttä 2020 tutkimushanketta. Verkkopuolustusta lähestytään sekä tiedonsiirto- että suojaustekniikoiden kautta.

Jormakan tekemät yhteenvedot eri skenaarioissa osoittavat, että puolustustehtävä on haastellinen, mutta ei mahdoton. Puolustuksen onnistuminen edellyttää, että puolustaja pysyy mukana alan kehityksessä. Paikallaan pysyminen ja täten hyökkääjistä jälkeenjääminen aiheuttaa ajan kuluessa väistämättä aukkoja puolustusjärjestelmiin. Kehityksessa mukana pysyminen edellyttää riittäviä talous- ja henkilöstöresursseja.

6.5 Lopuksi

Suomea pidetään tietoyhteiskuntana. Internet-liittyminen ja matkapuhelimien määrässä olemme väkiluvun suhteen maailman kärkimaita. Meillä myös uskotaan hyvinkin voimakkasti teknisiin välineisiin ja niiden ylivoimaan. Samalla monasti unohdetaan teknisiin ratkaisuihin sisältyvät turvallisuusriskit.

Miten yhteiskunnan pitäisi suojautua verkkosotaa vastaan ? Tällä hetkellä meillä on monia toimijoita, kuten liikenne- ja viestintäministeriö ja sen alaisuudessa Viestintävirasto. Suojelupoliisilla on oma roolinsa, kuten myös Puolustustaloudellisen Suunnittelukunnan eri jaostoilla ja pooleilla. Yritykset ovat käytännön suojautumisessa ratkaisevassa asemassa.

Tämän hankkeen aikana on noussut esille kysymys, pitäisikö maahamme perustaa erillinen verkkoturvallisuusorganisaatio ja erillisiä CERT-tiimejä. Yhdysvalloissa vuonna 2000 perustettiin organisaatio hyökkäykselliseen tietoverkkosodankäyntiin (CNA). Yksi peruste hankkia hyökkäyksellisiä välineitä, kuten taisteluhelikopteri, on se, että täten me opimme toimimaan kyseisiä välineitä vastaan. Yksi pääkysymyksiä onkin, kenellä Suomessa pitäisi olla verkkohyökkäyksiin liittyvä osaaminen, jotta kykenemme harjoittelemaan puolustusta ennen kaikkea tulevaisuuden kriiseja varten.

Vai onko meidän lähettävä nykyisen kaltaisesta ratkaisusta, jossa jokainen toimija vastaa itse omista ratkaisuistaan ja omasta puolustuksestaan. Joka tapauksessa niin siviiliyrityksiin kuin Puolustusvoimiin pyritaan vaikuttamaan esimerkiksi samanlaisilla viruksilla. Omaan haasteensa muodostaa mikä olisi verkkoturvallisuusorganisaation toimivalta. Olisiko kyseisellä organisaatiolla kriittisissä tilanteissa oikeus käskeä esimerkiksi katkaisemaan kaikki ulkomaailmaan menevät yhteydet.

Verkkotaistelu 2020 - hanketta käynnistettäessa tiedostettiin, että hankkeella kyetään vain raapaisemaan aiheen pintaa. Hankkeen suurin tavoite on käynnistää keskustelua verkkotaistelusta sekä miten tämän maan niin julkiyhteisöjen kuin yritystenkin verkkoja tulisi puolustaa. Tutkimuksen aikana on noussut esille muutamia tutkimusalueita, joita tulevaisuudessa kannattaisi tutkia. Toivottavasti tämä julkaisu on helpottamassa asiasta kiinnostuneiden tutkimusten aloittamista ja auttaa ideoinnissa pidemmälle niissä suunnissa, joissa nyt ei onnistuttu liikkumaan.

Viime aikaisissa kriiseissä silmäänpistävä piirre on ollut tappioiden välttäminen. Sodankäynnistä on medioiden välityksellä luotu kuva jonkinlaisena videopelinä. Myös verkkotaistelun liittyy sama piirre. Lisäksi verkkotaistelu mielletään vain syrjäänvetäytyneiden nuorten miesten toiminnaksi. Tällä kirjalla on pyritty osoittamaan tämä käsitystä vääräksi. Verkkotaistelulla voidaan saavuttaa hyvinkin merkittäviä tavoitteita ja se on varmasti yksi tulevaisuuden taistelumuodoista. Tämän kirjan tekijät haluavat korostaa, että verkkotaisteluiden käyminen ei poista sitä tosiasiaa, että tulevaisuudessakin sodankäyntiin kuluu myös aseellisten joukkojen välinen toiminta.

7. KRITIIKKIPUHEENVUORO – VERKKOTAISTELUT "TEKNIIKASTA TAKTIIKKAAN" – TIELLÄ ?

Jari Rantapelkonen
majuri,
Pääesikunta, johtamisjärjestelmäosasto

Jukka-Pekka Virtanen
majuri, viestitaktiikan opettaja
Maanpuolustuskorkeakoulu, Taktiikan laitos

> **Ajastaan jäljellejääminen ei millään muulla alalla ole rangaissut itse itseään niin katkerasti kuin sotataidon ja siinä juuri taktiikan alalla.**
> *Aaro Pajari, 1923*

Tässä julkaisussa, maavoimaesikunnan toisen vaiheen osatutkimuksessa kuvattu verkkotaistelu on väline eikä päämäärä. Välinettä on varauduttava käyttämään taistelujen ehkäisemiseksi ja tarvittaessa niiden käymiseksi. Aivan samoin kuin sotatieteen tärkein tehtävä on sodankäynnin kuvan muodostaminen voidaan ajatella, että taktiikan tutkimuksen tärkein tehtävä on taisteluiden kuvan muodostaminen[1]. Tässä tutkimuksessa tähän vaativaan tehtävään on rohkeasti tartuttu. Toimeenpantujen harjoitusten (Tieto 2000/2002), koetun käytännön (tietoturvaloukkaukset) ja tämänkin tulevaisuuteen katsovan tutkimustehtävän perusteella voi sanoa, että jonkinlainen muutos on jo meneillään. Epävarmuus taisteluiden kuvista lienee ikuinen ongelma.

Tämän päivän verkkotaistelut muistuttavat lähtökohtaisesti enemmänkin satunnaisia ilkivaltayrityksiä, hakkereiden kokeiluja tai rikollista järjestäytynyttä toimintaa kuin vakavaa sodankäyntiä. Osana sodankäynnin kokonaisuutta ne ovat olleet lähinnä alkeellisia yrityksiä vaikuttaa. Toisaalta esimerkiksi tiedusteluun tietoverkoissa on tänä päivänä suhtauduttava jo vakavasti. On myös huomattava, että verkkosodankäyntiin liittyvää tiedustelua ei välttämättä tehdä verkoissa. Tämä ei suinkaan poista sitä, että verkoissa sotilaallisesti organisoituna ei jo olisi potentiaalia aikaan saada vakavia vaikutuksia yhteiskunnan puolustamiseen valmistautuvalle asevoimalle. Varsinkin kun "hyökkäykset ovat muuttumassa harmittomasta hakkeroinnista kokonaisten yhteisöjen koordinoiduiksi ja johdetuiksi hyökkäysoperaatioiksi"[2].

Tietoturvallisuusasioiden neuvottelukunnan ehdotus Suomen kansalliseksi tietoturvastrategiaksi on yksi osoitus paitsi tietotekniikan ja tietopalveluiden hyödyntämisen lisääntymisestä niin myös verkkoihin liittyvien riskien vakavasti ottamisesta valtionhallinnon tasolla. Sotilaallisessa kehyksessä Natossa kehitetään verkko-operaatiokykyä, ja EU:ssa on kehitteillä verkko-operaatiokonsepteja. Informaatio-operaatioita on suunniteltu ja toteutettu niin sodankäynnin "tosi elämässä" kuin kotimaisissa harjoituksissa. Helsingin Sanomat julkaisi huhtikuussa uutisen, jossa Puolustusministeriön mukaan tietoverkkojen kautta leviävät informaatiouhat lisääntyvät[3]. Näiden tietoverkoissa etenevien uhkien torjuntaa varten perustetaan oma erityisyksikkö. Voidaan sanoa, että verkkosodankäyntiin erikoistuneita joukkoja koulutetaan jo järjestelmällisesti useissa maissa Euroopassa.

7.1. Verkkotaisteluiden kriittinen tarkastelu

Puolustusvoimien joukoissa varaudutaan verkkotaisteluihin myös taktisella tasolla. Informaatiosodankäyntiä organisoidaan Puolustusvoimissa samalla kun se on luokiteltu operatiiviseksi asiaksi. Informaatiolla vaikuttamisen merkitys strategisen iskun ennalta-ehkäisyvaiheessa on perinteistä sotilaallista uhkaa merkittävämpi.

Tässä Taktiikan laitoksen toimeenpanemassa verkkotaistelu –julkaisussa on vahva tekninen näkökulma. Itse asiassa koko sotahistoriaamme on johtamisjärjestelmien kehittämisessä vaivannut liiallinen teknisyys, mutta toisaalta samalla johtamisvälineiden puute. Liiallista teknisyyttä on päivitelty operatiivisten yleisjohtajien toimesta. Toisaalta teknisellä puolella on päivitelty taisteluiden johtajien pinnallista tietämystä tekniikasta. Tämä jännite onkin hedelmällinen lähtökohta innovatiivisen verkkotaisteluopin ja käytännön kehittämiseksi.

Tällaisen teknisen näkökulman ottamista verkkotaisteluihin puoltaa näkemys, jonka mukaan "viimeaikainen kiihkeä sotavarustelu on perin kiinteästi kytkeytynyt tekniikan soveltamiseen. Teknillisen kehityksen ripeä edistyminen on aiheuttanut sen, että sodankäynnin luonne on muuttumassa uudeksi, josta oikean kuvan saaminen vielä tällä hetkellä on epävarma."[4] Tämä silloisen kapteeni Veikko Sauran, tulevan sodan ajan viestipataljoonan komentajan ja everstin ajatuksien lainaus vuoden 1938 sotakorkeakoulun diplomityöstä osoittaa, että olemme sittenkin painimassa samantyyppisten sodankäynnin ilmiöön liittyvien ikuisuuskysymysten parissa. Toisaalta tekniikan nopeaa kehitystä voidaan pitää myyttinä. Ehkä olisikin parempi puhua sotilaallisten paineiden sijaan kaupallisista paineista tuottaa yhä nopeammin uusia tuotteita.

Käytännön kokemukset verkkotaisteluista Puolustusvoimien harjoituksissa osoittavat, että sota ja sodankäynti teknologisoituu. Onhan julkisuudessa keskusteltu 2000-luvulle siirryttäessä aina väitöskirjatasolla saakka teknoarmeijasta. Toki jo 1920 –luvulla puhuttiin "konearmeijasta aikamme iskusanana". Tässä tekniikan voittokulun nykyisessä ilmiössä on nähtävissä, että kehitys johtaa väistämättä informaatio- ja verkostosodankäyntikyvyn luomiseen paitsi yhteiskuntaan niin sen asevoimiin[5]. Informaatioon vaikuttaminen ja informaatiolla vaikuttaminen on osa taisteluita. Informaatiokamppailuja voidaan käydä myös ilman, että niihin liittyy perinteisen sotilaallisen voiman käyttöä. Tyypillisesti tällainen tilanne tulee kysymykseen esimerkiksi ennen ensimmäistä iskua, esimerkiksi strategista iskua, jossa verkko on taistelukenttä.

Tämä ei kuitenkaan vähennä tai poista vaan päinvastoin lisää sotilasjohtajien tarvetta saada "jotain tolkkua" johtamisjärjestelmien hallintaan. Muutoin näitä verkkoja ei voida käyttää tehokkaasti taisteluiden päämäärien edellyttämällä tavalla. Ilmaan jää kuitenkin kysymys miten sotilasjohtajien johtamiskulttuurin tällaisessa ympäristössä käy. Pitäisikö kaoottiselta tuntuva informaatioteknologia ottaa sotilaskäskyllä hallintaan? Vastaus löytyy luultavammin tältä väliltä. Olemme joka tapauksessa tilanteessa, jossa verkkotaistelut ovat ilmiönä tunkeutuneet taistelukentälle halusimmepa sitä tai emme. Taistelukentän kautta ne ovat tulleet tänne Maanpuolustuskorkeakoululle saakka, sotilasyhteisöön.

Näemmekin tämän kirjan osoituksena siitä, että maavoimat ja Taktiikan laitos pitävät asianaan pysyttäytyä informaatioajan taisteluista ajan tasalla. Ja eikä vain ajan tasalla vaan pyrkimyksenä edelleen kehittää joukkojamme kykeneväiseksi tällaiseen verkkotaisteluympäristöön. Taktiikan laitoksen pyrkimys saattaa uusi ilmiö julkisen keskusteluun on erinomainen lähtökohta saattaa suomalainen taisteluoppi nykyaikaisten vaatimusten tasolle. Voidaankin edelleen sanoa, että kun nykyiset Maanpuolustuskorkeakoulussa oppinsa saavat upseerit haluavat pysyä ajan tasalla ja palvella informaatioyhteiskunnan puolustusvoimissa, on upseerien tunnettava tekniikan tunkeutumisen merkitykset taistelukentällä. Tämä taistelukenttä tuntuu yhä enemmän muistuttavan kehitteillä olevaa taktista tietoverkkoa tai yhteiskunnan kriittisiä rakenteita, joiden toimivuudesta taistellaan ja joissa taistellaan.

Tämän artikkelin tarkoituksena on toimia edellisten kirjoitusten kritiikkipuheenvuorona[6]. Artikkelin kirjoittamisen lähtökohtana epäilemmekin tämän tutkimuksen kokonaisuutta, sen artikkeleiden lähtökohtia ja esitettyjä tutkimustuloksia. Toisaalta helmikuussa 2003 esitetyn seminaaripuheenvuoron tavoitteeksi asetettiin kirjoitusten mahdollinen parantaminen. Tämän artikkelin tavoitteena oli pyrkimys löytää muihin artikkeleihin nähden uutta näkökulmaa sekä siten myös luoda lukijalle kokonaisuuden arvioinnin kannalta ehkäpä parempia lähtökohtaedellytyksiä aiheen ymmärtämiseksi. Parhaiten lähtökohtiamme kuvaa mielestämme se, että pyrimme tällä kirjoituksella täydentämään edellisiä kirjoituksia ja herättämään kysymyksiä, joita ei muissa kirjoituksissa mahdollisesti ole huomioitu. Saattaahan olla, että artikkelien kirjoittajat ovat huomioineet esittämämme näkemykset, mutta he ovat jättäneet ne esimerkiksi rajauksista johtuen esittämättä. **Tarkoituksena** on näin ollen ennemminkin **kysyä ja ehdottaa asioita, joita voitaisiin jatkossa ottaa verkkotaistelututkimuksissa tai verkkotaisteluihin varautumisessa operatiivis-taktisella tasolla huomioon**.

Lähestymme muista poikkeavasti verkkosotaa **taktiikan näkökulmasta**. Siksi käytämmekin, joskin hyvin löyhästi, käsitettä verkkotaistelu. Sillä viittaamme niin Ahvenaisen käyttämään verkkosotaan kuin puolustusvoimissa käytössä olevaan tietojärjestelmäsodankäynnin käsitteeseen. Näemme taktiikan hieman toisin kuin esimerkiksi Maanpuolustuskorkeakoulussa tehdyssä virallisessa sotatieteiden määrittelyssä se nähdään. Taktiikka pelkkänä "oppina taisteluiden voittamisesta" on mielestämme ahdas ja käytännössä taktiikan todellisuutta vastaamaton määritelmä[7]. Taktiikka on ennen kaikkea ajattelua, jossa vihollisen toiminnan ja taisteluiden kulun arviointi sekä omien toimintavaihtoehtojen punnitseminen nousevat tärkeimmiksi kokonaisuuksiksi. Tekniikan rinnalle onkin mielestämme nostettava edelleen ajatukset taidosta käyttää joukkoja ja erilaisia välineitä tilanteiden vaatimalla soveltavalla ja innovatiivisella, suomalaisella tavalla.

Haasteeksi tämän artikkelin kriittisessä lähestymistavassa nousee se, että verkkotaistelut organisoituna taistelutoimintana on nykyisessä muodossa uusi asia. Esimerkiksi julkisia lähteitä ei ole juurikaan saatavilla. Se ei kuitenkaan merkitse etteikö tämäntyyppisestä verkkoilmiöstä olisi kokemuksia kerätty ja käytettävissä. Verkkotaistelukokemuksia löytyy ainakin puolustuksellisen tietojärjestelmäsodankäynnin ja siinä tietoturvallisuuden alalta sekä joistakin suurista Puolustusvoimien harjoituksista kuten Ilma 2002 –pääsotaharjoituksesta. Kokemukset liittyvätkin pääosin toiminnan tunnistamisen, suojaamisen ja puolustuksen järjestämiseen. Vaikuttamiseen liittyviä kokemuksia on, joskin ne ovat vähäisiä.

Sotilaiden on vaikea ollut tarttua tähän monimutkaiseen ja moniselitteiseen verkkotaisteluilmiöön. Se näkyy myös tässä kirjassa kirjoittajien valinnassa. Toisaalta kirjoittajien valinta osoittaa viisasta harkintaa, sillä mukaan on saatu Puolustusvoimien ulkopuolisia asiantuntijoita. Allekirjoittajien hankkima kokemus upseerinuralta esimerkiksi yhtymien viestitaktiikasta antaa toivon mukaan perspektiiviä, jotta tämän kritiikkikirjoituksen sanoma toimisi vakavasti otettavissa olevana kritiikkipuheenvuorona.

7.2. Käsitteellisiä jännitteitä

Verkkosodan nykyinen käsite on kaikkea muuta kuin selkeä ja yksiselitteinen lukuisine termeineen ja monisäikeisine määritelmineen. Verkkosotaan ja informaatioteknologiaan liittyvä käsitteistö on kulkenut pitkän tien lyhyessä ajassa. Selvyyttä käsitteistöön tuskin on aivan lähitulevaisuudessa näkyvissä. Käsitteiden sekamelskaan ja tulkinnallisuuteen onkin syytä tottua.

Sakari Ahvenainen on kirjoittanut verkkosodan historiasta ja käsitteen kehittymisestä amerikkalaisista lähtökohdista. Yhdysvallat on toiminutkin monien viimeaikaisten käsitteiden veturina. Tässä mielessä sillä on kiistatta suuri vaikutus ei pelkästään kirjoittajaan vaan voidaan sanoa, että Yhdysvalloilla on "informaatioylivoima" koko läntisestä maailmasta.

Sota ja taistelut ovat kuitenkin kulttuurin tuotteita myös globaalissa maailmassa. Siksi ainakin lyhyt katsaus suomalaisen verkkosodankäynnin ja verkkotaisteluiden käsitteiden juuriin olisi ollut paikallaan. Puolustusvoimissa on käytössä esimerkiksi käsite tietojärjestelmäsodankäynti[8], josta Ahvenainen on tietoinen viitatessaan siihen. Sellaiset kysymykset kuin miksi kyseiseen termiin on päädytty, mitä kautta ja mikä siihen on johtanut olisivat olleet kartoittamisen arvoisia.

Käsitteen sisältö koostuu muustakin kuin termistä. Tällainen käsiteanalyyttinen lähtökohta johtaa päätelmään, että koko verkkosodan historialla on pitemmät perinteet kuin artikkelissa kuvattu kymmenvuotinen "historia" vuodesta 1993 alkaen. Meille "kenttäviestimiehille" verkkotaisteluihin liittyville käsitteille löytyy käsiteanalyyttisesti kotimaiset juuret itsenäistymisaikojen alusta. Puolustusvoimissa siirryttiin kenttäviestitasolla viestiyhteysajattelusta verkkoajatteluun jo 40-luvulla, ja siitä järjestelmäajatteluun 80-luvun lopulla. Ajattelu oli hyvin suoraan sidottu teknisiin välineisiin. Olemmeko nyt palaamassa verkkotaisteluajattelussamme siis 80-luvulle?[9]

Toki verkkotaistelut nähdään kirjoituksessa huomattavasti laajempana ilmiönä. Verkkosodankäynnin määritelmällinen laajuus on jopa liian suuri, jotta niihin voisi taktisella tasolla konkreettisemmin tarttua. Verkkosodankäynnin käsitteiden kirjoituksesta voi kuitenkin tehdä päätelmän, jossa tietoverkot ovat oleellinen osa taisteluita. Tällainen käsitteellinen lähtökohta oikeuttaa tietoyhteiskunnan verkkojen puolustamisen sotilaallisin keinoin. Menemättä enempää lakitulkintoihin ja eettisiin kysymyksiin siitä onko kysymys sodasta, sotilaallisesta voimankäytöstä tai tietoverkkopalveluista, tulisi käsiteanalyysissä jatkossa perusteellisemmin argumentoida miksi tietoverkoissa tapahtuvaa toimintaa pitäisi yleensäkään määrittää sodaksi tai taisteluiksi. Maanpuolustuskorkeakoulussa tehtävissä tutkimuksessa valmiuslain oleellisimpien kohtien tarkastelu informaatiosodankäyntiin liittyen tulisikin ottaa tutkittavien asioiden listoille. Ja siellä mielestämme yhdeksi tärkeimmistä tutkimustehtävistä.

Strategisen iskun uhkakuvaan varautumisen kannalta päätelmä on antoisa. Sillä vaikuttamiseen pyritään ja sotilaalliseen vaikutukseen kyetään eittämättä pelkästään tietojärjestelmäsodankäynnin keinoin. Näin tiedustelusta ja valmiudesta vastaavien huomio ei pelkästään kohdistu "raudan" seuraamiseen. Verkkojen ja tietoyhteiskunnan puolustuksesta vastaaville nousee kuitenkin esiin kysymys: mitä jos muutkin artikkelissa kuvatut verkkosodankäynnin toiminnot kohdistetaan informaatioyhteiskuntaamme? Ahvenaisen mukaan kun tietojärjestelmäsodankäynti on "yhdeksäsosa verkkosodan nykyisestä sisällöstä".

Tutkimuksellisesti näitä käsitesuhteiden avaamista on hedelmällistä jatkaa – varsinkin suomalaisten jo käytössä olevien käsitteiden osalta. Toisaalta myös suomalaisten käsitteiden vertaaminen ulkomaisiin käsitteisiin on kansainvälisen yhteensopivuuden kehittämisen aikana on tärkeää. Verkkotaistelukykyä kehitettäessä onkin syytä herättää kysymys siitä pitäisikö meidän ottaa kansainväliset käsitteet sellaisinaan, kehitämmekö käsitteet täysin omiin tarkoituksiimme kansalliselta pohjalta vai kehitämmekö käsitteistöä suuntaan, joka on "jotain siltä väliltä". Saako teorian ja käytännön välillä olla suuria eroja? Voidaan myös ajatella, että verkkotaistelu -käsitteen epäselvyys on voimavara, joka antaa mahdollisuuden innovaatioihin, sillä tiukka määritelmä ei ainakaan rajoita taistelutekniikan ja taktiikan kehittäjiä. Toisaalta tiukempi määritelmä ohjaa toimintaa täsmällisemmin ja tehokkaammin, kun pyrkimyksenä on nostaa joukkojen verkkotaistelusuorituskykyä.

Ehdottammekin, että verkkotaistelu –käsitettä tuleekin jatkossa rajata selkeämmin. Samalla se on määritettävä meitä suomalaisia lähemmäksi. Tämä antaisi aiheen käsittelylle lisää syvyyttä. Samalla se loisi myös tiiviimmät lähtökohdat verkkotaistelukonseptin kehittämiseksi. Tarkempi konteksti ja näkökulma verkkotaistelukäsitteeseen toimii hedelmällisenä jatkona verkkotaistelukeskustelun jatkamiseksi Maanpuolustuskorkeakoulussa ja laajemmin myös Suomessa. Tärkeää olisikin löytää käsitteitä, jotka palvelevat innovatiivisen verkkotaisteluopin kehittämiseksi. Käsitteiden suoran lainaamisen etuja ja haittoja onkin siinä yhteydessä puntaroitava perusteellisesti.

Verkkotaistelukäsite on nopeasti sidottava lähemmin Suomeen ja suomalaiseen valmiuslainsäädäntöön. Kun Ahvenainen pitää verkkotaisteluita osana sodankäyntiä, niin olisi mielenkiintoista ollut erityisesti lukea tutkijan käsityksistä voimasta ja voimankäytöstä sekä sen liittämisestä strategisen iskun ennaltaehkäisyyn ja torjuntaan tai mieluummin "harmaaseen vaiheeseen" sekä visioon vaikuttamisesta taistelukentällä vuonna 2020.

Tämä ensin mainittu olisi tuonut ainakin Maanpuolustuskorkeakoulussa opiskelevalle käsiteanalyysiä hieman lähemmäksi omaa kokemusmaailmaa. Samalla se olisi avannut käsitteeseen liittyviä ongelmallisuuksia esimerkiksi valtuuksista ja tulevaisuuden sodankäynnistä etiikkaa myöden. On tietysti totta, että tällainen pohdinta vaatii varmasti vähintään itsenäisen artikkeliavauksen. Suotavaa olisi nähdä aiheesta myös kokonaisen kirjan mittaisia pohdintoja.

Verkkosodan historia ja käsitteen kehittyminen –luvussa onkin hyvää se, että siinä ei ole pyrittykään lopulliseen määritelmään. Taktiikan ilmiöitä tarkasteltaessa on hyvä muistuttaa, että vaikka täsmällisten käsitteiden perään huudetaan, niin käsitteet eivät ole määritelmiä, jotka lopettavat keskustelun. Jos se ei sitten satu nimenomaisena tarkoituksena olemaan. Taktikko ajattelee kuitenkin taistelua juuri käsittein. Ainakin tieteellisesti tarkasteltuna on hyvä pyrkiä täsmällisiin, selviin, yksinkertaisiin ja totuudenmukaisiin käsitteisiin. Verkkosodan käsite on hedelmällinen, sillä verkoissa oleva ilmiö on kyetty verkkotaistelukäsitteen myötä nimeämään ja sille on kyetty tässä kirjassa antamaan merkityksiä. Se kuinka paljon koko kirja selventää ilmiön merkitystä taisteluiden osana ei ole kuitenkaan suuri. Tärkeää on jo se, että verkkotaisteluiden ilmiötä verkoissa sinällään on jo avattu. Tätä kautta ne tulevat meille ymmärrettävämmiksi.

7.3. Tiedon aika

Nykyisellään eri viranomaiset ja Puolustusvoimat ovat toteuttaneet tietoliikenneratkaisunsa itsenäisesti omin toimenpitein. Nämä erilliset ratkaisut ovat tukeutuneet teleoperaattoreiden palveluihin. Puolustusvoimilla on käytössään oma kiinteä ja yhteensopiva televerkko, joka on kriisissä ja sodassa huomattava etu.

Viranomaisyhteistyön toteuttaminen tällaisessa tietoliikenneympäristössä on kuitenkin haaste. Esimerkiksi monet turvallisuusviranomaisten sensoriverkot kuten tutka- ja kameravalvonta tai liikkeen ilmaisevat sensoriverkot eivät ole kaikilta osiltaan yhteensopivia. Kuitenkin turvallisuusviranomaisten yhteistyö ja yhteistoiminta on päivittäistä. Tietojen pitäisikin siirtyä joustavasti, ei pelkästään eri viranomaisten välillä, vaan eri viranomaisten ja organisaatioiden väleillä. Pelkästään erilaisten tilannekuvien muodostaminen vaatii sitä. Tämä on yksi syy siihen, miksi on tärkeää määrittää verkkotaisteluihin liittyviä yhteisiä peruskäsitteitä kuten datan, informaation ja tiedon käsitteitä.

"Tiedon merkitys Suomen puolustamisessa" –kirjoitus on tärkeä ja tarpeellinen. Tampereen tietojohtamisen tutkijat professorin johdolla avaavat siinä näitä informaation, datan ja tiedon sekä kriittisen infrastruktuurin käsitteitä. Käsitteet eivät ole kuitenkaan mekaanisia irrallaan verkkotaisteluiden ilmiöstä ja verkkotaistelijoista, jolloin onkin aiheellista kysyä miten esimerkiksi taisteluissa helposti pintaan nousevat tunteet liittyvät näihin käsitteisiin.

Vaikka verkkotaisteluiden käytäntöä ajatellen kirjoitus tarjoaa taustatietoa, niin se ei juurikaan tarjoa taktikoille, joukoille tai tekniikan kehittäjille uusia sovellettavia ajatuksia. Kysymmekin olisiko verkkotaistelussa tiedon, informaation ja datan erittelyn sijaan mielekkäämpää analysoida tiedon eheyttä, käytettävyyttä ja luottamuksellisuutta laajemmin. Tiedon käytettävyyteen liittyy keskeisesti pohdinta operaatioiden turvallisuudesta. Ainakin taisteluiden operatiiviselle johdolle on merkityksellisempää tietää ovatko tiedot saatavilla ja voiko niihin luottaa.

Tuija Helokunnas, Terhi Laukkanen ja Kalle Viitanen kirjoittavat, että "tietoverkot ovat osa kriittistä infrastruktuuria, ne tarjoavat hyökkäävälle taholle sekä käyttökelpoista tietoa että välineen yhteiskunnan toimintaan vaikuttamiseksi"[10]. Tämä johdattaa verkkotaisteluissa mukana olijan kysymään itseltään tärkeän kysymyksen: mistä verkoista ja tiedoista olen tällä sodankäynnin tasolla riippuvainen. Mitkä ja missä ovat ne kriittiset tiedot, joita operatiivinen johtaja tarvitsee tai verkkotaisteluissa menestymiseksi tarvitaan? Mitä tietoja verkkotaisteluissa tarvitaan, jotta niiden suojaamiseen kyetään keskittymään? Verkkotaistelijalle ja sen joukolle saattaakin paljastua, että nuo tärkeät ja kriittiset tiedot eivät olekaan enää omissa käsissä vaan muualla; ylemmän johtoportaan esimerkiksi noissa Pohjoisen Maanpuolustusalueen tietovoimaloissa.

Puolustajan kannalta tuleekin Kalevi Halosen mukaan tunnistaa kriittisen tiedon osalta se mikä tieto on viholliselle tärkeä sen pyrkiessä tavoitteisiinsa. Haasteena on se, että tällaista tietoa ei voi vain sotilaallisesti ajatelmaviivoin luetella. Kysymyksessä on paremminkin tilanteenmukainen analyysi- ja ajatusprosessi.[11]

Helposti näihin kysymyksiin mitä tietoa tarvitaan ja milloin annetaan vastaukseksi - verkkotaisteluiden suunnittelusta ja toteutuksesta vastaaville mahdoton tehtävä - kaikki mahdollinen tieto ja jatkuvasti. Miten tällaiseen vaatimukseen suhtautuu ja miten siihen pitäisi suhtautua esimerkiksi Pohjoisen Maanpuolustusalueen tietovoimaloista vastaavien?

Avataksemme hieman tätä kysymystä voidaan ajatella, että informaatiosodankäyntiin ja verkkotaisteluihin liittyviä tietoja, joita tarvitaan voivat olla valtakunnallisella tasolla esimerkiksi sähkömagneettisen spektrin käyttöön liittyvät olosuhde- ja valvontatiedot sekä tiedot valtakunnallisista tieto- ja sähköverkkojen toimivuudesta. Muita tietoja voisivat olla esimerkiksi tiedot tunkeutumisyrityksistä, virushälytyksistä ja haittaohjelmien käytöstä sekä elintärkeiden toimintojen ja tietojen turvaamisesta. Monet yhteiskunnan verkoissa ja taisteluhengessä tapahtuvat muutokset heijastuvat ja vaikuttavat suoraan Puolustusvoimien kykyyn taistella verkoissa.

Alueellisella tasolla verkkotaistelijat tarvitsevat tietoja myös alueellisen sähköverkon toiminnasta ja tietoliikenneverkoista. Yhtymätason verkkotaisteluissa on tärkeää tietää muun muassa paristojen, varavoimakoneiden, polttoaineiden ja tietojenkäsittelylaitteiden ja ohjelmistojen tilasta sekä paljonko niitä on reservissä sekä kuinka nopeasti ne olisivat käyttöönotettavissa.

Asetettu kysymys tiedon tarpeista on vaativa, koska vastauksissa varmaankin nousee esille eri johtoportaiden ja toimijoiden hyvinkin erilaiset tarpeet. Lisäksi tiedon tarpeet ovat sidoksissa taistelutilanteisiin. Eri vaiheissa tarvitaan erilaista tietoa. Tiedon tarpeellisuus on siis suhteellinen ja dynaaminen ilmiö. "Tiedon merkitys korostuu" –hokeman sijaan väittämää on syytä jatkossa perustella tieteellisemmin osoittaen esimerkiksi mitkä faktat ja tekijät osoittavat sen käytännössä todeksi. Taktisella tasolla on syytä porautua edellä mainittujen tiedon eheyden ja käytettävyyden kysymyksiin.

Juuri tällaiseen problematiikkaan olisi tutkijoilla ja tutkimuksella varmasti annettavaa. Puolustusvoimissa etsitään erilaisissa tilannekuvien kehittämisprojekteissa vastauksia juuri tämäntyyppisiin tiedon tarpeisiin. Usein kuitenkin törmätään kysymyksiin, joihin kukaan ei kykene juuri edellä mainitusta tiedon suhteellisuudesta ja dynaamisuudesta

johtuen löytämään vastauksia. Taisteluista vastaavan operatiivisen johdon on kyettävä yksilöidymmin asettamaan vaatimuksia operaatioiden turvallisuudelle. Se edellyttää heiltä nykyistä syvällisempää käsitystä informaatiosta ja informaatiosodasta.

OODA-luupin esiin nostaminen on aiheellista, mutta sitä kohtaan olisi voinut esittää kritiikkiä. OODA-luuppi nimenomaan nostaa korostetusti ajan merkityksen, jota "tiedon merkitys Suomen puolustukselle" -kirjoituksessa ei yllättäen juurikaan käsitellä. Ajan käsitteen liittäminen tiedon tarpeisiin on nähdäksemme aivan keskeinen tutkimuskysymys, joka tulisi purkaa auki. Tiedon ja ajan suhde nostaa verkkotaisteluissa tiedon käytettävyyden ja eheyden kysymykset uudelleen esille. Esimerkiksi Tieto 2000 –harjoituskokemusten mukaan "pahin tapa ei olekaan tuhota operatiivisia tietoja vaan vääristää tai varastaa niitä"[12]. Kysymys siitä milloin on tiedon aika lienee ikuinen, mutta verkkotaisteluissa erittäin tarpeellinen ja ajankohtainen. Se on tutkimuksellisesti ainakin sotilasyhteisössä toistaiseksi valitettavan vähän pohdittu kysymys.

Kysymys siitä milloin eri tietojen tulee olla saatavilla ja missä aikaikkunassa niillä on merkitystä on harjoituksissa koettu tärkeäksi asiaksi. Se on näkynyt muun muassa komentajien ja taisteluiden johtajien huutoina reaaliaikaisen tilannekuvan perään. Teknisesti reaaliaikainen tietoverkko ei kuitenkaan takaa sitä, että tieto siinä olisi reaaliaikaista. Kysymmekin onko tämä koko reaaliaikaisen tilannekuvan tarve sittenkin myytti. Esimerkiksi kokemukset LIRVA.C –viruksen leviämisen estämisestä verkkoympäristössä nosti ajan merkityksen arvioimisen jälleen tärkeäksi tekijäksi. Puolustaja pyrkii estämään verkoissa olevien tietojen saastumisen reagoimalla tilanteeseen mahdollisimman nopeasti. Saastumisen vaikuttavuus kun on sitä laajempi mitä kauemmin viruksen annettaan levitä.

Tiedon merkitystä pohtivassa artikkelissa nostetaan ihmisen merkitys esille, mutta vain sivulauseessa. LIRVA.C –virustapauksessa saattoi aistia sen, että tärkein tieto oli sittenkin ihmisillä päässä. Datan ja informaation tarpeet eivät olleetkaan välittömiä. Vaikutukset reaaliaikaiseen viestintään olivat vähäisiä varsinkin kun sähköpostiliikenteen sijaan välttämättömimmät asiat hoidettiin muutoin eikä todella merkittäviä asioita oltu sidottu verkkoihin[13].

Kuinka kauan esimerkiksi yhtymän siirtyvä operaatiokeskus (SOKE) voi olla ilman yhteyksiä verkkoon verkkokeskeisessä sodankäynnin mallissa, että sen vaikutukset alkaisivat näkymään yhtymän taisteluissa? Millä tavalla vaikutukset näkyisivät? Mikä on sen tiedon tarpeen ajallinen merkitys, jota maanpuolustusalueen tietoverkoissa välitetään? Mitä vaatimuksia näille verkoille sitten asetetaan? Mitä tietoja tietoverkkoihin ei kannata tallentaa? Tällainen pohdiskelu antaisi lisäarvoa keskusteluun verkottuneen informaatioyhteiskunnan kehittämiseksi tai vaikkapa tulevaisuuden vuoden 2020 taistelukentällä toimivan yhtymän teknisten ratkaisujen, taistelutekniikan ja taktiikan kestävämmälle kehittämiselle.

"Tiedon merkitys Suomen puolustamisessa" –kirjoitus herättää varmasti jo otsikollaan huomiota. Kirjoitus on tarpeellinen avaus ja ravistelee Maanpuolustuskorkeakoulun koulutus- ja tutkimusyhteisöä pohtimaan ympäristön muutosten vaikutuksia omaan toimintaan. Kirjoituksessa paljastuu implisiittisesti se, että organisaatiotasoilla tiedon muodostamisessa ei ehkä ole samanlaista merkitystä kuin tavanomaisessa sodassa, jossa tieto tuli suoraan hierarkista ketjua ylhäältä alas ja päinvastoin. Mikä on tällaisen mahdollisen päätelmän vaikutus johtamiselle, yhteistyölle ja itse taisteluille vuonna 2020?

Aiheen käsittely johtaa pohtimaan kysymystä sen johtopäätöksistä. Esimerkiksi VTM Paulus Maasalo kirjoittaa ensimmäisen vaiheen tutkimuksessa informaation ja teknologian suhteesta ja sen merkityksestä länsimaisen yhteiskunnan kriisinsietokykyyn seuraavaa: "voidaan vain spekuloida kuinka riippuvaiseksi ihminen... tulee koneista ja informaatiojärjestelmistä"[14]. Maasalo ehdottaakin, että "tiedon merkityksen" -mantran laajenemisen sijaan tulisi kyseenalaistaa se mistä oikein on kysymys: yksilön, yhteisön, Suomen vai EU:n haavoittuvuudesta. Jos sähköt ovat poikki niin kaatuuko tietokone, ihminen, kaupunki vai koko valtio ja mitkä ovat seuraukset. Todelliseksi haavoittuvuudeksi tarjotaan ajatusta, jossa ihmiset menettävät perusolemuksensa; inhimillisyyden ja sitä kautta mahdollisesti toimintakyvyn. Informaatiojärjestelmien totaalisuus kun tuo – itse asiassa on jo tuonut - erittäin suuren mahdollisuuden paitsi manipuloida todellisuutta niin valvoa yksityisyyttä.

Tiedon merkitys Suomen puolustamisessa kirjoituksen keskeisin päätelmä on juuri tuo informaatioriippuvuuden kasvaminen. On tärkeää, että sen positiivisten ja negatiivisten seurausten purkamisen merkitystä suoalaiselle yhteiskunnalle ja sen Puolustusvoimille avattaisiin jatkotutkimuksissa. Voidaanko joukkojemme ja sen yksilöiden tekemisiä seurata ja valvoa sekä niihin vaikuttaa jostakin kaukaa tietokonepäätteen takaa? Entä muualta kuin tietokoneverkoista? Miten? Ja entä sitten?

7.4. Taistelutekniikasta verkkopuolustustaktiikkaan

Professori Jorma Jormakka ja tutkimuspäällikkö Mikko Hyppönen ajattelevat, että verkkotaisteluja voidaan käydä samoista lähtökohdista kuin tavanomaisempia taisteluja. Taktikoille tämä antaa erinomaisen lähtökohdan lähestyä verkkotaisteluita. Sillä kun verkkotaisteluihin pätevät suurin piirtein samat sodankäynnin periaatteet kuin muissakin sodankäynnin ulottuvuuksissa; maalla, merellä ja ilmassa sekä "pehmeämmässä" informaatioulottuvuudessa, on niitä operaatioita suunnittelevien ja arvioijien helpompi ajatuksellisesti lähestyä.

Verkkotaisteluita käydään tietoverkoissa, kyberavaruudessa. Sillä tarkoitetaan tässä puheenvuorossa suhteellista informaatioteknologiaan perustuvaa tilaa, jossa vihollinen on epämääräinen, taistelut usein näkymättömiä ja jossa taisteluiden voittamiseen pyritään teknologisen edun turvin. Verkkotaisteluita voidaan käydä niin prikaatin tietoverkoissa, puolustusvoimien verkoissa kuin suomalaisen yhteiskunnan tietoverkoissa ja globaalissa Internetissä.

Verkkotaistelutapa näyttäytyy ja heijastuu Suomessa sen tietoverkko-, tietoturva- ja yleensäkin teknologiapolitiikasta eli Suomen tavasta toimia ja tuottaa hyvinvointia tietoverkkojen avulla ja niillä. Verkkosota tässä mielessä reflektoituu meidän kansallisesta tyylistä, jota toki kansainvälistyminen haastaa. Turvallisuusviranomaisten välillä jo toimivien ja kehitteillä olevien viranomaisverkkojen yksi keskeisimmistä haasteista ei liity suoraan kuitenkaan välineisiin ja verkkoihin vaan hallinnonalojen johtamiskulttuuriin sekä tapoihin johtaa niissä ilmeneviä verkkotaisteluja eri hallinnonaloilla. Sama pätee myös pienemmässä mittakaavassa yhtymiin. Perinteinen sotilaallinen johtamiskulttuuri törmää helposti informaatioteknologian alalla vallitsevaan kulttuuriin ja päinvastoin.

Mitä verkkotaisteluissa pitäisi sitten johtaa? Tietoako? Kuinka tuota tietoa johdetaan, kun sen käyttö estetään tai tiedon sisällölliset muutokset ravistelevat taistelevaa jouk-

koa? Emme malta olla ottamatta esille tietoturvayhtiö F-Securen toimitusjohtaja Risto Siilasmaan sanoja johtamisesta. Siilasmaan kokemuksen mukaan ihmiset ovat ainoa resurssi, vain ihmisiä voi johtaa[15]. Tutkimuksellisesti tällainen ajattelu merkitsee väistämättä, kun verkkotaisteluiden sodan kitkan halutaan voittaa, niin tekniikan, taktiikan kuin johtamisen laitosten taisteluihin liittyvän tutkimuksellisen yhteistyön tiivistämistä.

Samalla näin luodaan hyvät edellytykset testata ja kehittää nykyistä suunnittelu- ja johtamisprosessia. Kuinka verkkotaistelut otetaan tuossa prosessissa huomioon ja miten verkkotaistelut tukevat operatiivisia päämääriä? Pitääkö prosessia muuttaa suuntaan tai toiseen? Vai kykenemmekö hoitamaan verkkotaistelut ilmiön vain sillä, että se lisätään pelkästään viestipäällikön tehtäväluetteloon?

Verkkotaistelutapojen rutinoitumiseen on matkaa. Hyppönen kuvaa pirteästi jatkuvan ja kiihtyvän muutoksen problematiikkaa. Verkkotaisteluopin pysyvyyttä haastaa verkkojen, ohjelmistojen ja välineiden siviilivetoisuus, jossa kaupallisuus heijastuu läpi yhteiskunnan myös verkkotaisteluopin ja tapojen kehittämiseen. Tätä oppia ei voi pelkästään sotilaskäskyin kehittää ja pitää hanskassa. Tarvitaan siis laajempaa tahtoa, joka löytyy yhteisistä ja ensisijaisesti kansallisista tarpeista.

Verkottuneella tietoyhteiskunnalla tulee olla yhteinen puolustuskonsepti. Puolustuskonseptissa on tärkeää, että se kykenee vastaamaan taistelukentän valmisteluun, ennakkovaroituksen saamiseen sekä taisteluiden käymiseen liittyviin kysymyksiin. Luotu rauhanaikainen malli CERT-FI:n, viranomaisten ja yritysten tietojen vaihdosta on erinomainen lähtökohta kehittää myös sodan ajan mallia. Se ei tietystikään saisi poiketa juurikaan rauhan aikaisista toimintatavoista.

Verkottuneen tietoyhteiskunnan puolustamiskonseptiksi tietoverkoissa on tarjottu "syvän puolustuksen konseptia". Syvä verkkopuolustuskonsepti perustuu ajatukseen, jossa verkot koostuvat kerrostuneista verkko- ja tietorakenteista sekä ihmisistä. Tuntuu selvälle, että tällaisen konseptissa nousee tärkeäksi kyky yhteistoimintaan. Puolustusvoimien valmiuspäällikkö, prikaatikenraali Ari Puheloinen, toi esille asian tärkeyden Tieto 2000 –harjoituksen päätöstilaisuudessa. Puheloisen mukaan yhteiskunnan voimavarojen ja eri alojen tietämyksen yhdistäminen on järkevää[16]. Tämä ei kuitenkaan poista sitä, että jokaisen itsenäisen organisaation on kyettävä taistelemaan eristäytyneenä. "Yhdessä mutta tarvittaessa erikseen" toimii vaativana ohjaavana ajatuksena ja suunnan näyttäjänä verkkotaistelukonseptin kehittämiseksi.

Verkkopuolustus ei ole lainkaan syvää, jos torjunta tapahtuu vain palomuurilla tai virustarkistuksina työasemilla. Laajemmin ajateltuna haasteellista oman syvän puolustuksen konseptin kehittämisessä on kyky omaksua uusia tekniikoita. Vaikka Suomea pidetäänkin tietoliikennelaboratoriona, on verkkotaisteluoppia kehitettäessä ymmärrettävä, että organisaatiollinen kehitys, sen toimintatavat ja ohjeet eivät pysy tämän kehityksen perässä. Olemme organisaationa siis aina tekniikan kehityksestä jäljessä askeleen verran - myös vuonna 2020.

On huomattava, että aitoa syvää verkkopuolustuskonseptia kehitettäessä riippuvuus ulkomaalaisista laitteista ja ohjelmistoista on ongelma. Sillä näiden tuotteiden turvallisuustestaukset ja evaluointi ei ole samalla tasolla kuin sen toivoisimme olevan. Testaukset vaativat suurehkoja resursseja. Eikä huoltovarmuus varsinkaan laitepuolella pitkän kriisin

aikana ole helposti saavutettavissa.

Taistelukentän valmistelemisessa pitkälle tulevaisuuteen on tärkeä olla tietoinen tekniikan kehittymistä. Professori Jormakan verkkopuolustusartikkelissa tätä kuvataan seikkaperäisesti. Mutta mitä sitten? Menemättä enempää tähän verkottumiskehitykseen ja riippuvaisuuteen tietoverkkoinfrastruktuurista, on jatkossa avattava sen merkityksiä verkkotaisteluihin valmistautuvalle puolustajalle[17]. Millaisia mahdollisia ongelmia niistä voi aiheutua operaatioille? Mitä ongelmille voitaisiin tehdä etukäteen varautumisen puitteissa?

Verkkopuolustus –artikkelin ansio on sen verkkotaistelukentän elementtien selkeässä kuvaamisessa. Verkkotaistelut matojen, viruksien ja palomuurien maailmassa antaa harhaanjohtavan kuvan verkkotaisteluista mikäli lukija ei kykene liittämään sitä laajemmin taistelukenttään. Ikään kuin niissä olisi kysymys jostain maagisesta myyttisestä tekniikan ilmiöstä. Verkkotaisteluiden "heikoin lenkki" on kuten Heikoin lenkki –ohjelmassa ihminen. Hienot ja ylelliset ohjelmistosovellukset uusimpine päivityksineen eivät ole mitään jos ihminen jätetään verkkotaisteluissa huomiotta. Siksi onkin syytä korostaa, että tietoisuus (tämä kirja) ja kouluttautuminen (MpKK:n opetussuunnitelmat) sekä taktiikan kehittäminen (harjoitukset ja tutkimukset) ovat jopa tärkeämpiä kuin tekniset verkkosodankäynnin ratkaisut. Pitäisikö tiedon eheyden puolustamisen kysymys siis nostaakin voimakkaammin sille kuuluvaan asemaan?

Kevin Mitnick on kirjoittanut kuinka yritykset syytävät suurimman osan turvallisuusbudjeteistaan välineisiin ja korkeaan teknologiaan, mutta samaan aikaan ne eivät kouluta ihmisiään. Mitnick kertoo esimerkin kuinka hän sai taidoillaan tärkeää informaatiota yrityksestä, joka ei suostunut sitä myymään hänelle edes suuresta summasta:
Tein töitä lakiasianajotoimistolle Denverissä. Olin hyvin kiinnostunut langattomasta teknologiasta. Minulla oli Motorola kännykkä ja halusin purkaa sen osiin ja katsoa oliko siinä mitään haavoittuvuuksia. Päätin hankkia lähdekoodin. Yritykset pitävät tätä koodia hyvin arvokkaana. Sitä ei voi vain ostaa. Sille on omistusoikeus. Kävellessäni kotiin soitin Motorolan 1-800 numeroon. Kun olin lopettelemassa 20 minuuttia kestävää kävelyäni kotiin, minulla oli tuo lähdekoodi yksinkertaisesti vain käytettyäni puhelinta ja puhelahjoja. Ajatelkaa kuinka paljon rahaa ja kehittynyttä turvallisuustekniikkaa Motorola on käyttänyt suojatakseen tuon koodin.[18]

Jorma Kajavan mukaan sosiaalinen hakkerointi on Suomessakin yksi tärkeimpiä turvallisuusuhkia, joka tulisi ottaa vakavasti. Sosiaalinen hakkerointi perustuu vakuuttavaan käytökseen, jossa herkkäuskoisia ihmisiä huijataan tai ihmisiä yleensä ohjataan vaikuttajan haluamaan päämäärään. Se kun on helpompaa ja halvempaa tietomurtautumista kuin teknisten rakenteiden kautta hyökkääminen. Henkilöstön valmennuksen kautta on mahdollisuus nostaa tietoturvakulttuurin tasoa.[19]

Sisäpiiriläisen luokittelussa viholliseksi on muistutettava, että suomalaisten hyväuskoisuus voi koitua kohtaloksi. Toisaalta taas verkkotaisteluissa tarvittava "miehistö" ja taisteluiden operaatioympäristössä toimivat tuntevat Suomessa pääosin henkilökohtaisesti toisensa. Siksi sisäpiiriläisten värvääminen on Suomessa vaikeaa. Hyppösen kuvaamat aktivistit ja haktivistit vihollisina eivät jää paljastumatta, mutta ovat siitä huolimatta verkkojen ylläpitäjille uhka.

Hyppösen ja Jormakan sekä Mitnickin ja Kajavan sanomiset herättävät kysymään tiedämmekö me, verkkojoukkomme ja muut sodan ajan joukkomme, mitä tietoa verkoista luovutetaan, mitä saa luovuttaa ja kenelle. Tiedämmekö mitä tietoa yhtymän tai maanpuolustusalueen verkoista on saatavilla ja mitä niihin on tallennettu?

Hyökkääjän kasvottomuus monine uhkineen on puolustajalle haaste, taistelipa hän internetissä, viranomaisverkoissa, puolustusvoimien omissa verkoissa tai taktisen tietoverkon taistelukentällä. Siksi on äärimmäisen tärkeää, että – vaikkakaan elektronisen sodankäynnin uhkia ei olekaan tarkasteltu – kaikki taktisen tietoverkon taistelukentällä taistelevat ovat tietoisia puolustuksen järjestämismahdollisuuksista sekä vaikuttamiskeinoista.

Tämä vihollisen kasvottomuus ei ole kuitenkaan uusi ilmiö. Tynkkysen mukaan taktiikan kehittäminen oli heti sotien jälkeen hankalaa, koska todennäköinen vihollinen oli jo silloin muuttunut jossain määrin hahmottomaksi[20]. Sotilaallisessa toiminnassa tulee aina olla selkeä päämäärä. Päämäärä edellyttää vihollista, ainakin kuviteltua vihollista, joka on määritelty ja jonka toimintatavat ainakin osin tunnetaan. Voimmeko taistella ilman vihollista? Onko tekniikasta sinänsä jo tullut vihollinen, joka estää tai hidastaa toimiamme? Kuinka puolustan ja hyökkään artikkeleissa tosin osoitetaan, että tekniikan muuntumisen vauhti riittää jo sinällään ilman tällaista filosofista pohdintaa vihollisesta. Tällainen hahmottomuus on juuri verkkotaisteluun kuuluva ominaispiirre.

Vihollisen lisäksi nousee samainen keskeinen kysymys puolustus- ja hyökkäysartikkeleja lukiessa pintaan kuin verkkosota-artikkelia lukiessa. Mikä verkkotaisteluissa on rikos, entä taistelutoimi? Onko tietoturvaloukkaus taistelutoimi? Mikä on yksittäinen tapahtuma, jota ryhdytään joukon toimesta järjestelmällisemmin selvittämään ja käsittelemään? Nämä ovat oikeutettuja peruskysymyksiä, kun olemme vielä uuden asian kanssa tekemisessä ja sitä kehittämässä. Ehkäpä juuri siksi taktiikan perusteelliselle pohdinnalle on erityinen mahdollisuus.

Operatiivisen johdon on tärkeä tietää millaisia vaikutuksia verkkotaisteluilla on taistelevan joukon toimintaan. Siksi häiriöiden, taistelujen seurauksien ja vaikutusten suuruuksien arvioiminen sekä merkitys turvallisuudelle on syytä tuoda esille. Verkkotaisteluvalmiuteen liittyvät toimenpiteet ja verkkoturvallisuuden parantamiseksi tehtävät toimenpiteet lukeutuvat varmasti hyökkäysten aikana sarjaan "operatiiviselle johtoportaalle ilmoitettavat asiat". Tämä edellyttää kuitenkin käsitystä siitä mihin koko verkkopuolustus ja vihollisen torjuminen perustuu.

Jormakan ja Hyppösen artikkelit antavat teknisiä perusteita taktiikan kehittämiseksi. Niistä voi päätellä, että erityisesti verkkotaisteluissa ennakoinnin merkitys nousee keskeiseksi. Eikö juuri tällöin pitäisi teknisten arviointien lisäksi tehdä erilaisia taktisia tilanteenarviointeja? Vaikka nyt saattaisi tuntua, että Suomella on verkkotaisteluissa "materiaalinen ylivoima" mahdollisesta vastustajasta, niin juuri innovatiivinen taktiikka luo mahdollisuudet vieläkin suuremmille voitoille – aivan talvisodan mottitaktiikan mallin mukaan. Taistelut ovat ennen kaikkea taktiikkaa, kykyä ajatella.

Kun verkoissa ryhdytään taktikoimaan, on taktiikasta ja taistelusta puhuttaessa pohdittava tavoitteita. Mitä puolustetaan? Mihin vihollinen hyökkää? Missä on painopiste? Kuinka vihollista harhautetaan? Missä on reservi? Mitkä ovat meidän ja hyökkääjän voiman

lähteet? Mikä on tavoiteltava loppuasetelma? Esimerkiksi Miettisen ja Pakarisen mukaan on tärkeää, että "tiedustelu- ja hyökkäysyritykset harhautetaan toisaalle". Heidän mukaansa eräänä taisteluteknisen tason keinona voidaan käyttää valepalvelimia, kun halutaan antaa väärä käsitys omasta toiminnasta ja kiinnittää vihollisen huomio toisaalle. Mitä muuten merkitsee taktiikan ja taisteluopin kehittämiselle päätelmä, että "tietokoneiden harhauttamisesta tulee paljon vaikeampi tehtävä kuin ihmisten harhauttamisesta"?[21]

Jos taktiikka on ajattelun lisäksi myös taitoa, niin mitä se oikein tarkoittaa verkkotaisteluissa. Taito on kykyä ajatella verkkotaistelua taktisesti siten, että jo hallittuja perusteita sovelletaan uusiin taktisiin kehyksiin yllätyksellisissä tilanteissa. Taitoa ei siis voi liittää pelkistetysti mihinkään taktisiin määritelmiin siitäkin syystä, että suomalaisille upseereille on kautta sotahistorian ollut tyypillistä hylätä sääntöihin sovitettu sotataito. Näin he ovat pitäneet itsellään toimintavapauden. Mutta miten verkkotaktista taitoa oikein voi mitata? Taktiikka kun määrittyy lopulta aina ja yhä uudelleen tilanteenmukaisesti jokaisessa taistelussa erikseen. Ovatko nämä taidot Ahvenaisen ja Helokunnaksen ym. esille tuomia käsitteellisen ajattelun taitoja, Jormakan kuvaamia teknisten trendien hahmottamisen kykyjä vai Hyppösen kuvaamia hyökkäystekniikoiden hallintaa ja niiltä suojautumista? Varmaa on, että verkkotaisteluiden taktiikan kehittämistä ei määritä mikään yksittäinen tekijä. Voidaan kuitenkin sanoa, että taidoilla on tässä "maailmassa" erityinen arvo.[22]

Verkkopuolustusta ja verkkohyökkäystä käsittelevissä artikkeleissa ollaan Markku Iskaniuksen ajatuksien linjoilla, jossa operaatiotaidon ja taktiikan tutkimus tähtää käytännöllisiin tavoitteisiin. Nämä kirjoitukset antavat perusteita verkkotaistelutaktiikan periaatteiden sekä verkkotaisteluissa tarvittavien toimintamenetelmien, järjestelmien ja organisaatioiden kehittämiselle.[23]

7.5. Kohti innovatiivista verkkotaistelutaktiikkaa

Tämän kriittisen puheenvuoron tarkoituksena on ollut täydentää muita puheenvuoroja ja nostaa esille joitakin pohdinnanarvoisia kysymyksiä. Siten meillä on ollut mahdollisuus kohottaa teknisen ja taisteluteknisen tarkastelun rinnalle kysymyksiä taktiikan perimmäisestä olemuksesta. Kysymykseen vastaaminen edellyttää tässä kirjassa tuotujen verkkotaisteluiden oppiosaan perehtymisen lisäksi pohdintoja ja tutkimuksia siitä mitä taktisia taitoja verkkotaistelu vaatii, miten ne ilmenevät verkkotaisteluissa ja miten taktiikkaa voidaan edelleen kehittää. Verkkotaistelu, huolimatta massiivisista etukäteisvalmisteluista, saattaa kulminoitua, niin kuin monet taistelut aiemminkin, kykyyn soveltaa sodankäynnin ikuisia periaatteita taistelutilanteen mukaan.

Kokonaisuuden kriittisesti tarkastelemiseksi on ensimmäiseksi tehtävä kysymys tämän tutkimuksen lähtökohdista, siitä miten tässä toisen vaiheen tutkimuksessa huomioitiin ensimmäisen vaiheen tutkimustulokset. Vastaus tähän kysymykseen jää epäselväksi. Sinänsä se ei tutkimuksen arvoa vähennä verkkotaisteluiden esiintuomiseksi. Asiakkaan (maavoimaesikunta) kannalta tämä voi herättää epäilyjä tutkimuksen käytettävyydestä. Tosin länsimaisen yhteiskunnan haavoittuvuus -tutkimuksen tuloksista voi päätellä verkottumisen ja informaation merkityksen korostuvan, jolloin verkkotaistelututkimukselle oli tilaus[24]. Mikä verkkotaisteluiden merkitys on asevoimille?

Ehkä Taktiikan laitoksen ja taktiikan kannalta vähiten huomiolle jäänyt ja samalla eniten jatkotutkimuksia vaativa asiakokonaisuus tässä kirjassa on taktiikan, verkkotaistelutaktiikan pohtiminen. Taistelut ovat enemmän kuin pelkkä oppi taisteluista. Taktiikka on nimenomaan ajattelua sekä taitoa. Verkkotaistelutaktiikan voi määritellä viestitaktiikan määritelmää mukaillen "verkkoon liittyvän kapasiteetin taidokkaaksi ohjaamiseksi verkkovoimaksi siten, että verkkovoima toimii yhtymän tavoitteen mukaisena taistelukertoimena[25].

Mutta kaikki aikanaan. Onko tällainen kritiikki liian aikaista? Sillä taktiikan kehittäminen vaatii aikaa, kyseenlaistamista, keskusteluja ja väittelyjä. Tämä kirjan kirjoittajien erilaiset kirjoitukset ja taustat ovat jo edistäneet sitä. Artikkelit osoittavat verkkotaisteluista kiinnostuneiden olevan oikealla tiellä.

Kysymmekin sen lisäksi mitä informaatioajan innovatiivinen verkkotaistelutaktiikka on kysymyksen mihin tämä verkkotaistelutaktiikka voisi perustua. Innovatiiviseen verkkotaistelutaktiikkaan kulkemisen tiellä haasteeksi voi nousta sen kokemusperäisen ominaispiirteen löytäminen ja luominen puolustusvoimiin. Saattaa olla, että se muodostuu aluksi yllättävän laajalle, mutta vain eriytyneelle osalle puolustusvoimia. Se ei saa merkitä sitä, että operatiivinen osa laiminlöisi sille elintärkeän kokonaisuuden, joka mahdollisesti rajoittaisi yllättävästi sen yleistä toimintavapautta operoida. Siksi sotaharjoituksissa on kaikkien operaatiopäälliköiden syytä etsiä itselleen mahdollisuuksia toimia esimerkiksi viestipäällikköinä tai tutkijoina. Kokemustutkimukselle löytyy näissäkin taisteluissa kunnianhimoiselle tutkijalle paikka[26]. Verkkotaisteluista ja niiden johtamisesta on teknikoiden ja taktikoiden yhdessä hankittava taistelukokemuksia, jotka tulee kirjata ylös ja levittää.

Vaikka verkkotaistelun oppiosan muodostaminen tämänkin kirjan tavoin löytää hyvin sille olennaisia verkkotaisteluun kuuluvia osia ja osin myös kaavamaisia "perusratkaisuja", niin vasta niiden soveltamista voidaan pitää varsinaisena taitona. Käytäntö onkin usein ajanut suomalaiset siirtymään kaavamaisista ratkaisuista kokeilemaan jotain toimivampaa, taidokkaampaa ja omaperäisempää.

Olisiko Maanpuolustuskorkeakoulun johtamisen laitoksen työnimellä "johtamisjärjestelmäkeskus 2004" paikka, joka voisi toimia johtamisjärjestelmäalan sotakeskuksena operatiivis-taktisella tasolla? Taktiikan laitoksen henkilöstö pääsisi näin ollen rohkealla virtuaaliaskeleen ottamisella tekniikan miesten ja naisten mukaan kehittämään malleja verkkotaisteluiden toteuttamiseksi. Tekniikka mahdollistaakin tietojärjestelmäsodankäynnin ja verkkotaisteluihin liittyvien taktisten sotapelien haltuun ottamisen. On tärkeää, että tällaisten mahdollisuuksien ja ominaisuuksien saamiseksi kyseiseen taisteluiden simulaatiokeskukseen pidetään huoli. Mekanistinen tekniikkaan perustuva malli sopii vain massiivisille suurarmeijoille.

Harjoitukset, joissa synnytetään arvokkaita omia taistelukokemuksia ovat arvokkaita paitsi kyseiselle joukolle niin verkkotaistelututkimukselle. Näin mahdollisuus luisua epätodelliselle pohjalle vähenee. Suurimpia ongelmia esimerkiksi ulkomaisten kokemusten seuraamisessa onkin se, että niissä keskitytään pelkästään Internetissä tänä päivänä toimivien vihollisten (pääosin 15-vuotiaiden script kid) touhuun. Omaa kokemusta ei kannatakaan laiminlyödä, vaan on rohkeasti tartuttava taktiikan kehittämiseen, jotta tämä sodankäynnin ulottuvuus - vallankumouksellinen siinä mielessä että sitä ei nykyisessä

mielessä ja merkityksessä ole aiemmin ollut – saa informaatioajan ansaitseman vakavan huomion taktiikassakin.

Verkkotaisteluita käsittelevien taktiikan tutkimuksien on siis kyettävä syventymään todellisiin verkoista juontuviin taktisiin ongelmiin. Tärkeää olisikin keskittyä todellisten vaikutusten analysoimiseen, arvioimiseen ja mittaamiseen verkoissa ja yhtymissä[27]. Yhteyksien menettämisen todellinen merkitys joukoillemme verkkotaistelukentällä pitäisi kyetä täsmällisemmin arvioimaan, olipa kysymys voimannäytöstä, ehkäisystä tai torjunnasta. Jokaisen sodan ajan joukon tulisikin asettaa itselleen kysymys: "kuinka kauan kykenemme operoimaan tehokkaasti ilman tietoverkkoja?". Onko taistelukenttä tämän kysymyksen suhteen erilainen vuonna 2020 kuin tänään?

Hyppönen kirjoittaa puheenvuorossaan, että "käytettävät tietokoneet pitäisi kokonaan eristää julkisista verkoista". Tämä rohkaisee kehittämään verkkotaistelutaktiikkaa suuntaan, jossa myös taktisella tasolla verkot kyetään eristämään tarvittaessa muista verkoista, olivatpa ne julkisia verkkoja, maanpuolustusalueen sotilasverkkoja tai taktisen tietoverkon osia. Näin voidaan kehittää myös kestävämpi verkkotaisteluoppi, joka palvelee välineenä eikä päämääränä Suomen puolustamisessa.

Toiseksi verkkotaisteluita käsiteltävien tutkimuksen on kyettävä vastaamaan siihen, millaisia taitoja komentajalla, operaatiopäälliköllä, esikunnalla ja verkkotaistelijoilla tulisi olla, jotta he kykenisivät menestyksekkäästi ennakoimaan tai ongelmat kohdatessaan ratkaisemaan ne - mielellään ennen kuin niitä taisteluissa kohdataan.

Taktiikkaa kannattaakin tulevaisuudessakin kehittää lähtökohdista, jossa mikään teknologia ei tee verkkotaistelusta turvallista. Vain harjaantuneet ihmiset ja verkkotaistelijat kykenevät takaamaan turvallisuuden. Mieleen tuleekin keskeinen ajatus Bruce Schneierin kirjasta: "If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology"[28]. Scneierin lause osuu kuin "nenä päähän". Analogiana todettakoon, että verkkotaisteluita ei voi voittaa pelkän teknologian avulla. Niin kauan kuin taistelu on sosiaalista toimintaa videopelien sijaan on keskityttävä niin tekniikan ja teknologian kuin taktisten taitojen sekä asenteiden kehittämiseen. Maanpuolustuskorkeakoululla on tässä vaativa ja tärkeä rooli.

Aaro Pajarin mukaan se joka "terävimmin on kyennyt arvostelemaan tulevan sodan taktillista luonnetta ja sen vaatimuksia koulutukseen nähden, on aina vähimmin saanut kokea epämieluisia yllätyksiä ja on parhaiten säästynyt raskaita uhreja maksavilta kokemusostoilta."[29] Taktiikan synnyttäminen tekniikan rinnalle onnistuu vain, kun ei jäädä lepäämään entisille laakereille. Verkkotaistelut –julkaisu osoittaa, että asiaan on rohkeasti tartuttu ja alan kehitystä seurataan vaikka käsitteet ja koko verkkotaistelukonsepti ovat uusina ja osin kypsymättöminä "sodan sumun" peitossa.

Ehkä yksi kirjan tärkeimpiä johtopäätöksiä on se, mihin Jormakka päätyy, että hyökkäyksiltä kokonaan suojautuminen ei ole mahdollista. Kun siihen yhdistää Kajavan ajatuksen, jossa valitettavan usein käytettävyys on tärkeämpää kuin turvallisuus30, niin voidaan ajatellakin Hyppösen tavoin, että on erityisen tärkeää kyetä eristämään verkot. Siksi puolustuksessa onkin erityisen tärkeää olla omavarainen. Mutta kuinka kauan, siinäpä kysymys. Toisaalta yhteisissä verkoissa herää myös artikkeleista heijastuva päätelmä, mitä tietoja yleensäkään kannattaa tietoverkkoihin tallentaa. COTS –tuotteilla taistelemi-

sen merkityksiä onkin avattava laajalti sillä turvallisuusviranomaiset pyrkivät Suomessa jatkossa sekä tiivistämään yhteistyötä että ottamaan kaupallisia tuotteita käyttöön sellaisenaan.

Suosittelemmekin, että verkkotaistelututkimusta jatketaan ja sitä täydennetään rivakasti. Tutkimuksena arvoisia kohteita voisivat olla nykyisen tietojärjestelmäsodankäynnin käsitteen tai sen mahdollisen seuraajan verkko-operaatioiden konseptin soveltava analysointi sekä käytännön taktiikan ja tekniikan asettamat vaatimukset ja mahdollisuudet verkkotaisteluihin liittyvälle tiedustelulle, valvonnalle, puolustukselle ja hyökkäykselle. Verkkotaistelutaktiikan kehittämisen tie osana informaatio-operaatioita saattaa olla pitkä ja kivinen[31]. Mielenkiintoisen ilahduksen toisi varmaan käytännönläheiset kirjoitukset esimerkiksi maanpuolustusalueen verkkokeskeisistä taisteluista, alueellisten viestijoukkojen ja viestipataljoonien toiminnasta verkoissa.

Strategisen iskun oppi on merkinnyt ratkaisevaa siirtymistä jalkaväen ja tykistön vaikutusten yhdistämisestä kohti tietoverkkojen yhdistämistä; kamppailua johtamisjärjestelmissä. Taistelualue on laajentunut ja siirtymässä metsäalueilta kohti informaatioympäristöä. Suomessakin informaatiosodankäyntiin ja verkkotaisteluihin osoitettuja joukkoja käytetään paitsi strategisen iskun ennaltaehkäisyyn niin muiden joukkojen sotilaallisen suorituskyvyn tukemiseksi ja parantamiseksi. Vie varmasti aikaa - emmekä ole ollenkaan varmoja tuleeko edes sellaista aikaa - jolloin verkkotaisteluun kykeneviä joukkoja käytetään taisteluissa ja sodassa "rikkomaan ja tuhoamaan paikkoja sekä tappamaan ihmisiä".

Ei tarvitse kuitenkaan odottaa edes vuoteen 2020, kun voi jo päätellä, että esimerkiksi strategisen iskun ennaltaehkäisyvaiheessa taistelut ovat kuitenkin "lähinnä bittien vihellystä ja virusten ujellusta tietoverkoissa ilman savua, tulta ja ihmistappioita"[32]. Tällaiselle tasolle taistelu ei kuitenkaan välttämättä jää vaikka sitä toivoisimmekin. Joka tapauksessa tapahtuivatpa veriset taistelut ennen tai jälkeen strategisen iskun tai jossain muussa muodossa vuonna 2020, sisältävät ne tämän verkkotaistelu-ulottuvuuden.

Meille tärkeät taktiset kysymykset syntyvät omista kokemuksista. Verkkotaistelut ovat osa muuta taistelutoimintaa. Ilman niitä on vaikea jatkossa kehittää suomalaista viimeisteltyä ja innovatiivista operaatiotaitoa ja taktiikkaa sekä verkkotaistelutaktiikkaa ja verkkotaistelutekniikkaa. Toinen vaihtoehto verkkotaistelutaktiikan kehittämiseksi on ottaa kokemukset ulkomailta annettuina - sitten joskus kun se ensin siellä kehittyy ja tulee julkiseksi.

Verkkotaistelut –kirjoitusten päätelmänä voi johtaa ajatuksen siitä, että verkkoja ei voida myöskään vuonna 2020 rakentaa aukottomiksi. Tämä on terve lähtökohta niin kaikille taistelukentän taktisille suunnitelmille kuin omaksua se yhtymien taisteluiden käymiseksi. Omia kokemuksia kannattaakin sotaharjoituksissa systemaattisesti etsiä, jotta tekniikkaan kyetään realistisesti myös taktiikassa suhtautumaan ilman tietämättömyydestä johtuvia optimistisia odotuksia ja turhaumia. Kokemukset luovat hyvät perusteet innovatiiviselle suomalaiselle verkkotaistelutaktiikalle verkkokeskeisissä taisteluissa. Verkot ovat Suomessa tulevaisuudessa "harmaan vaiheen" tärkeä taistelukenttä, jonka merkitys ei ainakaan verkostoyhteiskunnan puolustajallekaan vähene.

LÄHTEET

Halonen, Kalevi (2000). Operatiivinen turvallisuus. Teoksessa Saarelainen, Jorma ym. toimituskunta. Johtamissodankäynti. Taktiikan laitoksen johtamissodankäynnin seminaari 26.-27.10.2000. Helsinki: Maanpuolustuskorkeakoulun Taktiikan laitos, Julkaisusarja 2, Taktiikan asiatietoa n:o 2/2000, s.32-55.

Huhtinen, Aki; toim (2002). Länsimaisen yhteiskunnan kriisinsietokyky 2020. Taistelun kuvat 2020 1. vaiheen taustatutkimus. Maanpuolustuskorkeakoulun Johtamisen laitoksen julkaisusarja 2, artikkelikokoelmat n:o 7. Helsinki: Maanpuolustuskorkeakoulu.

Huhtinen, Aki & Rantapelkonen, Jari (2001). Taistelut, kokemus ja tieto. Näkemys sotatieteellisestä viestitaktiikasta. Riihimäki: Viestikoulu.

Huhtinen, Aki & Rantapelkonen, Jari (2000). Kriittinen viestitaktinen ajattelu – viestiyhteydestä operatiiviseen ajatteluun. Teoksessa Rantapelkonen, Jari & Liimatainen, Heikki & Rantapelkonen, Jari (2000). Informaatioajan viestitaktisia ajatuksia. Loimaa: Ev A.R. Saarmaan säätiö ja Viestikoulu, s.67-86.

Iskanius, Markku (1997). Operaatiotaidon ja taktiikan tutkimus sekä tutkimusmenetelmät. MpKK:n taktiikan laitoksen julkaisusarja 2, n:o 1/1997. Helsinki: Maanpuolustuskorkeakoulu.

Kajava, Jorma (2002). Vakuuttava käytös avaa ovet yritysten liikesalaisuuksiin. Social engineering henkilöturvallisuuden keskipisteessä. Viestimies 4 / 2002, s.17-20.

Keskiväli, Kari (2000). Verkkosodankäynti. Teoksessa Saarelainen, ym (2000). Johtamissodankäynti. Taktiikan laitoksen johtamissodankäynnin seminaari 26.-27.10.2000. Julkaisusarja 2, Taktiikan asiatietoa n:o 2/2000. Helsinki: Maanpuolustuskorkeakoulu, s.255-296.

Koli, Markku (1995). Koli, Markku (1995). Sodankäynnin ja taistelun kuva 2000. Julkaisusarja 2, n:o 1/1995, Helsinki: Maanpuolustuskorkeakoulu.

Kopytoff, Verne (2002). Ex-hacker shares secrets of deception. Mitnick says 'social engineers' play big role in cyber attacks. San Francisco Chronicle, October 28, 2002.

Maasalo, Paulus (2002). Teknologia ja informaatio – Vaikutuksia länsimaisen yhteiskunnan kriisinsietokykyyn. Teoksessa Huhtinen, Aki; toim (2002). Länsimaisen yhteiskunnan kriisinsietokyky 2020. Taistelun kuvat 2020 1. vaiheen taustatutkimus. Maanpuolustuskorkeakoulun Johtamisen laitoksen julkaisusarja 2, artikkelikokoelmat n:o 7. Helsinki: Maanpuolustuskorkeakoulu, s.137-214.

Miettinen, Eero & Pakarinen, Markku (2001). Harhauttaminen tietoverkoissa. Viestimies 2/2001, s.43-44.

Pajari, Aaro (1923). Rauhanajan kouluutus suhteessa sodan todellisuuteen. Suomen sotilasaikakauslehti 1923, s.1-13.

PEjojä-os (2001). PEjojä-os:n esittely Pv:n operaatiopäälliköille n:o R1741/12/D/II 27.9.2001. Helsinki: Pääesikunnan johtamisjärjestelmäosasto.

Perttu, Jukka (2003). Sodan ajan joukkoja tarkoitus vähentää rajusti. Tietoverkoissa etenevien uhkien torjuntaan oma yksikkö. Helsingin Sanomat, 7.4.2003.

Rantapelkonen, Jari (2000a). Mitä on viestitaktiikka? Teoksessa Liimatainen, Heikki & Rantapelkonen, Jari; toim. (2000). Informaatioajan viestitaktisia ajatuksia. Loimaa: Ev A.R. Saarmaan säätiö ja Viestikoulu, s.91-114.

Rantapelkonen, Jari (2000b). Informaatiosotaa Tieto 2000 –harjoituksessa: Tietoyhteiskuntaa puolustetaan yhdessä. Viestimies 4/2000, s.14-19.

Rattray, Gregory J (2001). Strategic Warfare in Cyberspace. Cambridge, Mass.: MIT Press.

Saura, V (1938). Missä määrin nykyinen viestijohto ja nykyiset viestijoukot (kokoonpano, kalusto ja liikuntavälineet) vastaavat tarkoitustaan meikäläisissä olosuhteissa. Sotakorkeakoulu, Y13. Helsinki: SArk.

Savisalo, Sauli (2001). Informaatiouhan vaikutus tietoyhteiskunnan tietoteknisiin järjestelmiin. Lisensiaatintyö 6.4.2001, Espoo: Teknillinen korkeakoulu.

Schneier, Bruce (2000). Secret & Lies. Digital Security in a Networked World. New York: John Wiley & Sons.

Siilasmaa, Risto (2001). Ihmiset ovat ainoa resurssi. Teoksessa Tulikoe. Ihmisten johtaminen sodan ja rauhan aikana. Suomen Reserviupseeriliiton julkaisu. Jyväskylä: Gummerus, s.258-269.

Tynkkynen, Vesa (2003). Muuttuva sodan kuva – tarvitaanko tutkimusta? Virkaanastujaisesitelmä. Helsinki: Maanpuolustuskorkeakoulu, 14.1.2003.

Tynkkynen, Vesa (1996). Hyökkäyksestä puolustukseen. Taktiikan kehittymisen ensimmäiset vuosikymmenet Suomessa. Maanpuolustuskorkeakoulun Taktiikan laitoksen julkaisusarja 1/1996. Joutsa.

[1] Vrt. Koli (1995), s.5.
[2] Savisalo (2001), s.II.
[3] Perttu (2003).
[4] Saura (1938). s.1.
[5] Vrt. Tynkkynen (2003). Myös taktiikan professori Vesa Tynkkynen kiinnitti tähän asiaan huomiota virkaanastujaisesitelmässään. Tähän samaiseen asiaan, jossa propagandistisen "revoluution" sijasta voitaisiinkin puhua evoluutiosta, joka yhdistää vanhaa ja uutta on keskusteltu paljonkin ja kriittisesti "sotilaallisten asioiden vallankumous" -retoriikan yhteydessä erityisesti 1990-luvulla informaatiosodankäyntiin liitettynä. Suomessa julkinen keskustelu on ollut laimeaa. On toki selvää, että Suomessa olosuhteet ovat muuttuneet tiedonvälityksen osalta ratkaisevasti. Kukapa ei olisi tänä päivänä riippuvainen verkoista, sähköposteista, kännyköistä ja tiedosta (reaaliaikaisesta tiedosta)? Samoin moni organisaatio on muuttunut informaatioympäristön ja informaatiouhan vaikutuksesta.
[6] Tämä puheenvuoro esitettiin lyhennettynä helmikuun alussa 2003 MpKK:n järjestämässä seminaarissa. Seminaarin jälkeen verkkotaistelut artikkelien kirjoittajilla jäi mahdollisuus tarkentaa kirjoituksiaan. Tässä kirjoituksessa on tartuttu pääosin niihin artikkeliversioihin, jotka olivat kritiikkipuheenvuoron käyttäjien käytettävissä helmikuun alussa.
[7] Esimerkiksi Maanpuolustuskorkeakoulun tutkimusjohtaja, professori Mikko Viitasalo määrittää Suomen sotatieteellisen seuran vuosijulkaisussa Tiede ja Ase n:o 60 taktiikan kapea-alaisesti opiksi taisteluiden voittamiseksi. Hän viittaa lainauksessaan MpKK:n virallisiin määritelmiin. Samantyyppisesti on entinen taktiikan laitoksen johtaja Markku Iskanius määrittänyt kirjoituksissaan taktiikkaa.
[8] PEjojä-os (2001).
Tietojärjestelmäsodankäynnillä tarkoitetaan omien tietojen, niitä käsittelevien tietojärjestelmien ja niiden käyttämän tiedonsiirron suojaamista sekä vaikuttamista vastustajan tietojärjestelmiin, tiedonsiirtoon ja niiden sisältämään tietoon. Tietoverkot ovat yksi tietojärjestelmä. Järjestelmä sisältää myös sitä käyttävän henkilöstön ja toimintatavat.
[9] Huhtinen & Rantapelkonen (2000), s.68-75.
[10] Samassa yhteydessä todetaan, että tiedon salaus on hyökkäyksen keino. Tätä näkemystä olisi mielenkiintoista hieman avata lisää mitä sillä itse asiassa tarkoitetaan.
[11] Halonen (2000), s.52.
[12] Rantapelkonen (2000b), s.14-19.
[13] Yksi tärkeimpiä verkkotaisteluihin liittyviä tutkittavia asioita on vaikuttavuuden analysoimista koskevat kysymykset.
[14] Maasalo (2002), s.203.
[15] Siilasmaa (2001).
[16] Rantapelkonen (2002b), s.19.
[17] Verkkotaistelutaktiikkaa suunnittelevalle ongelmaksi voi osoittautua asiantuntijan käyttämät täsmälliset lyhenteet. Toisaalta juuri se osoittaa millaisesta tiedosta verkkotaisteluilmiössä tulee olla tietoisia. Operatiivisen johdon toivomuksena on, että käsitteiden tulisi olla mahdollisimman lähellä tavallista kieltä. Juuri tätä asiaa

on pohdittava, jotta tekniikan ja taktiikan tekijät eivät erkanisi toisistaan liian kauas. Tätä vaaraa artikkelissa ehkäistäänkin tuomalla empiirinen ilmiö käytäntöön.

[18] Kopytoff (2002).

[19] Kajava (2002). Kajava käyttää termiä vakuuttava käytös sosiaalisen hakkeroinnin sijaan.

[20] Tynkkynen (1996).

[21] Miettinen & Pakarinen (2001), s.44.

[22] Vrt. Rantapelkonen (2000a).

[23] Iskanius (1997), s.10.

[24] Ks. esim. Huhtinen, toim (2002). Toisen vaiheen tutkimuksien tarkoituksena oli kritiikki huomioiden ottaa huomioon ensimmäisen vaiheen tutkimustulokset.

[25] Vrt. Rantapelkonen (2000a).

[26] Huhtinen & Rantapelkonen (2001).

[27] Vrt. Tieto 2000 –harjoituskokemukset informaatiosodan tutkimus ja koulutustarpeista. Ks. Rantapelkonen (2000b), s.16-17.

[28] Schneier (2000), xii.

[29] Pajari (1923), s.5.

[30] Kajava (2002), s.19.

[31] Vrt. Rattray (2002). Yhdysvaltain ilmavoimien everstiluutnantti Gregory Rattrayn mukaan informaatiosodankäyntikyvyn kehittäminen saattaa viedä yhtä kauan kuin strategisen pommittamiskyvyn kesti eli 50 –vuotta. Rattray komentaa (v. 2001) yksikköä nimeltä 23rd Information Operations Squadron Fort Meadessa, Marylandin osavaltiossa. Hän vastaa ilmavoimien informaatiosodankäyntiin liittyvän taktiikan kehittämisestä. Aiemmin hän palveli puolustuksellisen informaatiosodankäyntidivisioonan apulaispäällikkönä ilmavoimien esikunnassa.

[32] Tynkkynen (2003). Tynkkynen on oikeassa siinä, että taistelukentän tulevaisuutta ei voi pelkästään rakentaa tällaisen varaan. Tämän ajatusmallin mukaan taistelukentän tulevaisuutta ei voi myöskään rakentaa pelkästään "jääkäriryhmä rynnäkössä itä-Suomen takametsissä" varaan. Taisteluihin kriittisesti suhtautuva löytäneekin tarpeellisen skenaarion tai niiden yhdistelmän näistä molemmista.

Maanpuolustuskorkeakoulu
National Defence College

ISBN 951-25-1423-0
ISSN 1238-2752